¿QUÉ SABEMOS DE?

Ciberseguridad

David Arroyo Guardeño,
Víctor Gayoso Martínez
y Luis Hernández Encinas

CSIC

CATARATA

¿QUÉ SABEMOS DE?

Ciberseguridad

David Arroyo Guardeño,
Víctor Gayoso Martínez
y Luis Hernández Encinas

CSIC

CATARATA

Ciberseguridad

David Arroyo Guardeño, Víctor Gayoso Martínez y Luis Hernández Encinas

Colección ¿Qué sabemos de?

COMITÉ EDITORIAL
Pilar Tigeras Sánchez, Directora
Carmen Guerrero Martínez, Secretaria
Pura Fernández Rodríguez
Enrique Barba Gómez
Arantza Chivite Vázquez
Javier Senén García
Carmen Viamonte Tortajada
Manuel de León Rodríguez
Isabel Varela Nieto
Alberto Casas González

CONSEJO ASESOR
José Ramón Urquijo Goitia
Avelino Corma Canós
Ginés Morata Pérez
Luis Calvo Calvo
Miguel Ferrer Baena
Eduardo Pardo de Guevara y Valdés
Víctor Manuel Orera Clemente
Pilar López Sancho
Pilar Goya Laza
Elena Castro Martínez
Rosina López-Alonso Fandiño
María Victoria Moreno Arribas
David Martín de Diego
Susana Marcos Celestino
Carlos Pedrós Alió
Matilde Barón Ayala
Pilar Herrero Fernández
Miguel Ángel Puig-Samper Mulero
Jaime Pérez del Val

Catálogo de publicaciones de la Administración General del Estado:

https://cpage.mpr.gob.es

Diseño gráfico de cubierta: Carlos Del Giudice

© David Arroyo Guardeño, Víctor Gayoso Martínez y Luis Hernández Encinas, 2020

© CSIC, 2020

http://editorial.csic.es

publ@csic.es

© Los Libros de la Catarata, 2020

Fuencarral, 70

28004 Madrid

Tel. 91 532 20 77

www.catarata.org

isbn (csic): 978-84-00-10713-0

isbn electrónico (csic): 978-84-00-10714-7

isbn (catarata): 978-84-1352-119-0

isbn electrónico (catarata): 978-84-1352-120-6

nipo: 833-20-179-5

nipo electrónico: 833-20-180-8

depósito legal: M-29.100-2020

thema: PDZ/UR/LNQE

Reservados todos los derechos por la legislación en materia de Propiedad Intelectual. Ni la totalidad ni parte de este libro, incluido el diseño de la cubierta, puede reproducirse, almacenarse o transmitirse en manera alguna por medio ya sea electrónico, químico, óptico, informático, de grabación o de fotocopia, sin permiso previo por escrito del Consejo Superior de Investigaciones Científicas y Los Libros de la Catarata. Las noticias, los asertos y las opiniones contenidos en esta obra son de la exclusiva responsabilidad del autor o autores. El Consejo Superior de Investigaciones Científicas y Los Libros de la Catarata, por su parte, solo se hacen responsables del interés científico de sus publicaciones.

Introducción

La progresiva tecnificación de nuestra sociedad se ha acentuado en los últimos 20 años, de forma que nos ha ido y nos va haciendo cada vez más tecnológicamente dependientes y vulnerables. Esta ambivalencia es especialmente significativa en el caso de las tecnologías de la información y de la comunicación (TIC). Desde la aparición del primer ordenador personal en 1981, nuestro tiempo ha sido testigo de la creación, despliegue y popularización de Internet. En efecto, la red forma parte del día a día de casi todos los ciudadanos del primer mundo. Hemos asumido el uso cotidiano de la ofimática, los teléfonos inteligentes y las redes sociales. La información digital y los medios de acceso a la misma configuran, pues, la interfaz preferencial de obtención, análisis e intercambio de conocimiento.

Esa digitalización de nuestro tiempo, por ejemplo, ha convertido las conversaciones familiares en intercambios de mensajes en grupos de WhatsApp, ha configurado las redes sociales como medio principal de acceso a las noticias en perjuicio de los medios tradicionales de información (periódico de papel, radio y televisión) y también ha posibilitado una gestión más automatizada y eficiente de recursos como el agua y la energía eléctrica. Consecuentemente, existe una imbricación de ese mundo artificial de intercambio y procesamiento de datos, el ciberespacio, en nuestro mundo físico. El ciberespacio no es un mero anexo del mundo real, sino uno de los elementos que actualmente lo configuran a través de una relación bidireccional que es de carácter problemático.

El trasvase operacional que existe entre el mundo físico y el ciberespacio convierte a las personas, empresas y organismos en usuarios de las cibertecnologías. Del mismo modo que hay acciones que pueden poner en peligro los intereses y derechos de los sujetos y agentes del mundo físico, también tendremos operaciones propias del ciberespacio que impiden que los usuarios vean satisfechas sus expectativas al usar cibertecnologías. Así, por ejemplo, el robo de un coche tiene su análogo en el robo de información de clientes en

plataformas de comercio electrónico, los secuestros de personas tienen su equivalente en el ransomware o secuestro de información, etc. Es más, hemos de tener en cuenta que los usos y abusos del ámbito cibernético tienen un impacto más allá del ciberespacio, tal y como se han puesto de manifiesto en incidentes de seguridad nacional e internacional como el famoso ataque Stuxnet, del que hablaremos más adelante. Dicho de otra forma, el ciberespacio no es simplemente un marco operativo, sino que se puede constituir en causa y efecto en el mundo físico por mor de los denominados sistemas ciberfísicos.

Por todo ello, hemos de hablar de ciberamenazas, ciberdelitos y del ciberriesgo como elementos de igual importancia que las amenazas, delitos y riesgos de nuestro mundo físico. En este sentido es de destacar el Convenio de Budapest (CETS nº185) sobre ciberdelincuencia (o convenio sobre cibercrimen), que es el primer tratado internacional que pretende hacer frente a los ciberdelitos[1]. Tal convenio es, de hecho, el único acuerdo internacional vinculante sobre este tema.

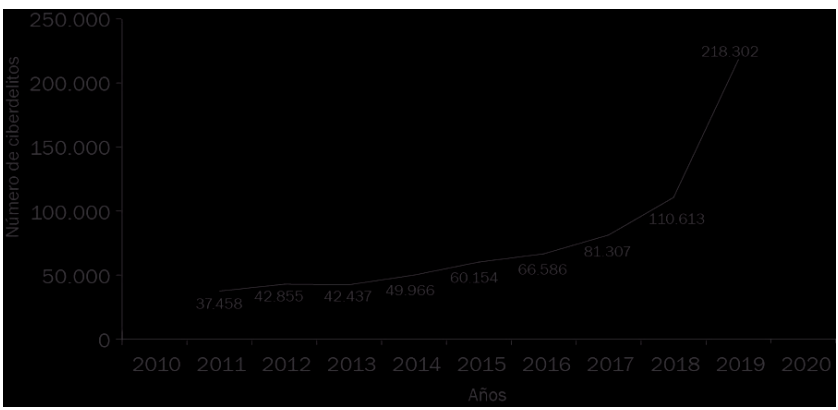
En la actualidad, hay más de 50 países que se han adherido al convenio. España lo firmó el 23 de noviembre de 2001 y lo ratificó el 1 de octubre de 2010. Tal ratificación ha tenido como consecuencia que, en la reforma del Código Penal español, de 2015, se introdujeran artículos para tipificar diferentes tipos de cibercrímenes, como el acceso no autorizado a sistemas informáticos.

Fruto de todo ello es la lucha constante de los Fuerzas y Cuerpos de Seguridad del Estado de España contra la ciberdelincuencia. Para tener una idea de la importancia de este tipo de delitos, cabe destacar el número de los mismos que se han llevado a cabo en los últimos años y su evolución creciente (figura 1). Así, solo en 2019 se cometieron 218.302 delitos, lo que representa el 10% de todos los delitos cometidos y supone un crecimiento del 35,81% respecto al año 2018. De todos ellos, 192.375 estuvieron relacionados con el fraude informático, 12.782 fueron amenazas y coacciones, se llevaron a cabo 4.275 falsificaciones informáticas y 4.004 accesos e interceptaciones ilícitas, 1.422 fueron delitos contra el honor,

1.774 delitos sexuales, 1.473 se relacionaron con la interferencia en los datos y en los sistemas, y 197 lo fueron contra la propiedad industrial/intelectual. Las tres comunidades autónomas con mayor índice de ciberdelitos fueron: Cataluña con 41.577, Madrid con 37.016 y Andalucía con 28.655.

Figura 1

Evolución del número de ciberdelitos entre 2011 y 2019.



Fuente: https://oedi.es/estadisticas/

Es de destacar que la mayor parte de estos delitos en 2019, un 88,1%, corresponden a fraudes informáticos o estafas, cuyo crecimiento en los últimos años ha sido muy destacable. Por el contrario, el número de delitos contra la salud pública ha ido disminuyendo paulatinamente, desde los 46 que se informaron en 2011, hasta llegar a 0 en 2015, valor que se ha mantenido hasta la fecha.

Según el VII Informe sobre Cibercriminalidad de la Secretaría de Estado de Seguridad (SES, 2020), de todos los delitos cometidos en

2019, se han resuelto unos 31.000 (algo menos del 15%), lo que permitió la investigación de cerca de 9.000 presuntos responsables. Según este informe, el perfil más común del ciberdelincuente en España es un varón de nacionalidad española de entre 26 y 40 años.

La ciberseguridad surge como mecanismo de control del ciberriesgo. De forma más precisa, podemos definir la ciberseguridad como el conjunto de técnicas, procedimientos y protocolos encaminados a la protección de la información vinculada a los usuarios de las cibertecnologías. Esta protección demanda la custodia no solo de la información en sí, sino también de todos los elementos precisos para su correcta gestión. Es decir, la ciberseguridad tiene como objetivo proteger todo tipo de activo o recurso de valor para una persona, empresa u organización.

De forma general, el ciudadano, las empresas y organizaciones se ven obligadas, en función de su especialización, a delegar parte de su confianza en los expertos que desarrollan herramientas y soluciones para proteger los activos mencionados. Ahora bien, esta cesión de confianza debe estar respaldada por un conjunto de soluciones que sean de fácil de uso y transparentes para los usuarios de las cibertecnologías. En efecto, un gran número de propuestas de seguridad han sido descartadas por los usuarios debido a su alta complejidad. Además, en el momento actual son muchos los servicios de gestión de información que han proporcionado casos concretos de abuso en el tratamiento de datos personales. En resumidas cuentas, la correcta implementación de la ciberseguridad debe combinar de modo equilibrado elementos de seguridad, de privacidad y de usabilidad.

La ciberseguridad es una ciencia de reciente cuño y que aún está por definir de modo preciso. Este libro pretende proporcionar una introducción al campo multidisciplinar de la ciberseguridad, y lo hace con una doble intención: pedagógica y de concienciación. Así, y como primer estadio del texto, se llevará a cabo un análisis de los principales recursos con los que contamos para generar, almacenar e intercambiar información en el ciberespacio. Todas esas modalidades de gestión de información determinarán distintos ámbitos de operación, a los que denominaremos dominios de la ciberseguridad. Cada uno de estos dominios reúne una serie de

rasgos específicos en lo relativo a las posibilidades de computación y gestión de información, pero también en lo concerniente a las ciberamenazas que afectan a sus activos de información. Así, no es lo mismo almacenar la información personal en el disco duro de nuestro ordenador en casa que hacerlo, por ejemplo, en Google Drive (es decir, 'la nube'). Además, es muy diferente acceder a la información desde nuestro ordenador, que hacerlo mediante un dispositivo móvil conectado a la wifi pública de un restaurante. También se introducirán las principales ciberamenazas de los distintos dominios de la ciberseguridad. La correcta concreción de tales amenazas se hará de acuerdo con las restricciones concretas de casos de uso en el ámbito personal, empresarial y gubernamental. Finalmente, el análisis de las ciberamenazas y su impacto se complementará con un resumen de mecanismos y procedimientos para la protección de los activos de información en el ciberespacio.

De forma más detallada, el libro consta de esta introducción y cuatro capítulos más. En el capítulo 1 se explicarán las principales ciberamenazas a la ciberseguridad de individuos y organizaciones. El capítulo 2 está dedicado a los dominios de la ciberseguridad, donde se discutirán las principales características, en términos de seguridad, de los ordenadores, los dispositivos móviles, la computación en la nube, el internet de las cosas (IoT, internet of things), etc. Una vez han sido introducidos los dominios que afectan a la gestión y procesamiento de información, en el capítulo 3 se presentarán los principales ámbitos de uso y aplicación de la ciberseguridad, es decir, la gestión personal y empresarial de la información, así como sus repercusiones sociales (uso de correo electrónico, mensajería instantánea, redes sociales, redes de comunicación, etc.). Cada uno de estos ámbitos de aplicación es susceptible de ser atacado en virtud de un uso negligente de las tecnologías o de sus posibles vulnerabilidades. En el capítulo 4 se incluye un conjunto de soluciones y recomendaciones a modo de guía de buenas prácticas para paliar en la media de lo posible el impacto de los ciberataques. Finalmente, el libro termina con el capítulo de conclusiones en el que se muestran aquellas relacionadas con los desafíos que supone la implantación de la ciberseguridad en nuestra sociedad.

Capítulo 1

Amenazas, vulnerabilidades y ataques

En este capítulo abordaremos dos de los principales conceptos relacionados con la seguridad: primero, las amenazas y los ataques a los sistemas y dispositivos que permiten la conexión a la red y que pueden poner en peligro los datos almacenados y transmitidos, llegando a vulnerar su confidencialidad, y segundo, la privacidad de los individuos, empresas y organismos.

La disciplina de la seguridad se encarga de proteger los activos de una organización o de un particular. Un activo es cualquier elemento que tiene valor para una organización o sujeto. Según el tipo de activo a proteger, estaremos tratando de seguridad de la información, seguridad de las TIC o ciberseguridad. En general, la seguridad de la información abarca todo aquello que tiene que ver con la protección de la información, ya sea almacenada o transmitida. Cuando la información se transmite, entonces se hace referencia a la seguridad TIC, en el sentido de que son las tecnologías de la información y las comunicaciones las encargadas de velar por los activos. Por su parte, la ciberseguridad no solo contempla la seguridad de la información que se transmite (momento en el que se interseca con la seguridad de la información), sino que contempla otros activos que no son solo información, pero que también pueden ser atacados por las TIC. Teniendo en cuenta esta distinción, para no abusar del lenguaje, a lo largo de este libro utilizaremos los términos "seguridad" y "ciberseguridad" como sinónimos, salvo que se especifique lo contrario. Por otra parte, no consideraremos la seguridad física, salvo cuando se diga expresamente.

La protección de los activos se realiza frente a la acción de los atacantes. Debe tenerse en cuenta que el objetivo de un atacante suele ser el de explotar las debilidades asociadas a

cualquier dispositivo que esté a su alcance (ordenador, teléfono, tableta, etc.) con el fin de sacar provecho a la vulneración de cualquiera de los tres objetivos principales relacionados con la seguridad de un sistema informático: confidencialidad, integridad y disponibilidad (CID). La confidencialidad garantiza la protección de la información de modo que sea secreta para quienes no tienen derecho a acceder a la misma. La integridad asegura la autenticidad de los datos almacenados, de modo que no puedan ser modificados, manipulados ni alterados por terceras partes sin permiso para ello. Finalmente, la disponibilidad de los datos almacenados en un sistema informático obliga a que su acceso sea posible en cualquier momento que sea solicitado por cualquier parte que esté autorizada a ello.

No obstante, el desarrollo de la tecnología ha obligado a ampliar los tres objetivos CID incluyendo el esquema de las tres reglas de oro (3Au): la autenticación, la autorización y la auditabilidad. La autenticación es una propiedad de la seguridad de la información que permite confirmar la identidad de un usuario y, eventualmente, la de sus dispositivos. En general, existen tres modos de autenticación: 1) algo que uno sabe (por ejemplo, una contraseña), 2) algo que uno tiene (una tarjeta inteligente, un pendrive, etc.), y 3) algo que uno es (huella digital, iris, geometría de la mano, etc.). Si solo se emplea una de las muchas características mencionadas, se dice que la autenticación es unimodal; mientras que, si son varios los factores empleados, se llama autenticación multimodal o multifactor (MFA, multi-factor authentication). La autorización es el proceso por el que se controla el acceso de un usuario a determinado servicio para realizar ciertas tareas. De este modo, una política de autorización señala lo que la identidad autorizada tiene permitido hacer, esto es, a qué recursos del sistema tiene acceso. La auditabilidad, por su parte, es la actividad que permite registrar y monitorizar la utilización de los distintos recursos. El registro de esta actividad es fundamental para validar el correcto funcionamiento de los sistemas de información y comunicación, así como para la identificación de fallas de seguridad y, cuando es posible, la depuración de

responsabilidades.

En el contexto actual, hemos de considerar, además, el derecho a la privacidad que tienen los usuarios de las TIC. En el dominio de los sistemas de información esta se puede entender como la capacidad que tiene un usuario de establecer quién, cómo y por cuánto tiempo un tercero puede explotar sus datos personales. En este sentido, la protección de privacidad implicará el consentimiento expreso de un usuario antes de que un tercero puede almacenar y procesar información sensible sobre su persona. Desde el punto de vista legal, en Europa, desde el 25 de mayo de 2018, el Reglamento General de Protección de Datos (RGPD) establece los mecanismos que se deben aplicar para que el tratamiento de la información personal sea congruente con el derecho a la privacidad del ciudadano.

Cualquier acción que comprometa alguno de estos objetivos de seguridad y privacidad se considera una amenaza, mientras que una vulnerabilidad es una debilidad en el sistema que puede ser explotada por una amenaza. En el Instituto Nacional de Estándares y Tecnología norteamericano (NIST, por sus siglas en inglés) puede consultarse la base de datos de vulnerabilidades (NIST, 2020).

Respecto a las amenazas, cabe precisar que pueden ser originadas por un ataque o ciberataque, por algún tipo de incidencia física (incendio, inundación, etc.) o por un descuido o negligencia en el seguimiento de recomendaciones de seguridad (usar en el ordenador del trabajo un pendrive personal). Por otro lado, las amenazas pueden estar originadas en el seno de una organización o tener su origen en el exterior.

La protección de una infraestructura TIC requiere identificar amenazas y establecer mecanismos de protección y contramedidas. Este proceso se concreta mediante una política de seguridad en la que se definen los recursos a proteger (instalaciones, equipos, puesta en marcha, reputación, etc.), para lo cual es preciso evaluar la importancia de cada uno de ellos, la probabilidad de que se vea afectado por la concreción de amenazas y el impacto de las mismas. Dicho de otro modo,

se ha de efectuar un análisis de (ciber)riesgos.

En término globales, es posible tener una idea del impacto de las incidencias de ciberseguridad a través de una estimación del coste económico que las fallas de seguridad, los ciberataques y los ciberdelitos han ocasionado a empresas y ciudadanos. Según el Observatorio Español de Delitos Informáticos, en 2019 el ciberdelito implicó pérdidas del orden de millones de euros a las víctimas. El informe de Accenture (2019) señala que, en los próximos cinco años, las empresas del sector privado corren el riesgo de perder alrededor de 5,2 billones de dólares debido a los ciberataques, lo cual es casi el tamaño de las economías de Francia, Italia y España juntas.

Como iremos viendo a lo largo del libro, el ritmo de aparición de amenazas y de nuevos actores en el ciberespacio no deja de crecer, lo que dificulta la construcción de una taxonomía de todos los posibles ataques existentes y de la forma en que son desplegados en los diversos entornos de aplicación. En lo que sigue, resumiremos los principales artefactos empleados por ciberatacantes (piratas informáticos o hackers[2]) y analistas de seguridad, en un caso para comprometer la seguridad de los sistemas, en el otro para validar la seguridad de los mismos. Asimismo, destacaremos un conjunto de organizaciones de gran interés para obtener información y apoyo en ciberseguridad.

Malware

La palabra malware hace referencia a todo tipo de software malicioso o dañino cuyo objetivo sea infectar ordenadores, tabletas o teléfonos móviles. El término “malware” (que procede de la unión de los términos malicious y software) fue utilizado por primera vez en 1990 por Yisrael Radai, debido a la aparición de nuevas modalidades de virus que hicieron necesario crear un término más general que pudiera incluir toda clase de software peligroso para los usuarios.

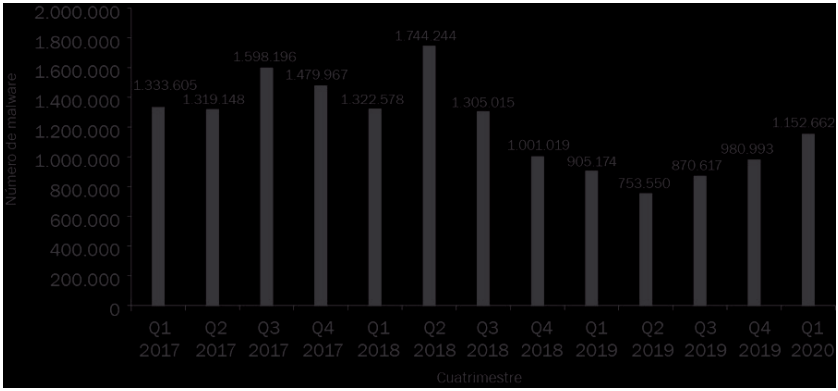
El rápido crecimiento de la industria informática a partir de la década de los setenta generó las condiciones para que surgieran los primeros virus informáticos, esto es, programas creados inicialmente para demostrar las capacidades de los programadores o con fines lúdicos, pero que con el tiempo se convirtieron en serias amenazas.

Los primeros virus seguían el mismo patrón: al ser ejecutado el programa en el que estaban ocultos, infectaban otros programas o incluso la parte del disco duro correspondiente al sector de arranque. Como los usuarios compartían aplicaciones informáticas mediante disquetes, los virus se extendían de forma lenta pero constante.

Algunos de los virus más conocidos a nivel mundial en aquella etapa fueron Brain (1986), Vienna (1987), Jerusalem/ Viernes 13 (1987), Casino (1991) o Michelangelo (1991). A finales de la década de 1980 habían sido detectados más de cien virus en el mundo, número que se incrementó exponencialmente en los siguientes años.

Figura 2

Evolución del número de malware informático.



Fuente: Kaspersky.

En el caso de España, además de los anteriormente mencionados, algunos de los virus más conocidos en aquella época fueron Flip (1990), también conocido como el virus de la renta y que colocaba los textos del ordenador boca abajo determinados días y horas, Anti-Telefónica (1990), que solicitaba tarifas telefónicas más bajas, o Barrotes (1992), que llenaba la pantalla de barras similares a las de las ventanas de las cárceles.

Con el inicio de la utilización masiva de Internet aparecieron nuevos virus con mayor capacidad de propagación. Así, en 1999 surgió el virus Melissa, que llegó a infectar más de 100.000 ordenadores en tan solo tres días.

Unos meses después, ya en el año 2000, se hizo famoso el virus I Love You, cuyo nombre se debe a que se propagaba mediante correos electrónicos que tenían como asunto esa frase. Este virus fue capaz de infectar más de 50 millones de ordenadores en todo el mundo.

Durante el siglo XXI han seguido surgiendo virus que, por sus efectos, han llegado a hacerse conocidos incluso fuera de los círculos de expertos. Algunos ejemplos son los virus Blaster (2003),

Sasser (2004), Storm (2007), Conficker (2008), Flashback (2011) y CryptoLocker (2013). En los últimos años, los casos más conocidos, acaparando titulares y telediarios, han sido Petya (2016) y WannaCry (2017), que infectó multitud de ordenadores de grandes empresas y obligó a algunas a detener su actividad mientras se procedía a su eliminación.

Fases de un ciberataque

Con el fin de protegerse contra los posibles ciberataques, los usuarios y las empresas deben conocer cómo se ejecutan estos ataques. Al ciclo de vida de un ciberataque se le conoce como cyber kill chain y, en general, no es lineal, sino cíclico, dado que al finalizar un ataque se puede estar en disposición de relanzar nuevos ataques sobre otras víctimas a las que se ha podido tener acceso durante el ataque realizado. Este ciclo de vida consta de los siguientes siete pasos (Hutchins et al., 2011):

Reconocimiento: el ciberatacante recaba toda la información que puede acerca de su objetivo, esto es, busca su información pública (web, redes sociales, etc.) e investiga sobre su tecnología, posible ciberdefensa (cortafuegos, sistemas de acceso, etc.). Con esta información valora si su ataque puede tener éxito o no y si procede a su intento.

Preparación: fase en la que se prepara el ataque elaborando el método a emplear, por ejemplo, un correo electrónico, preparación de un fichero, etc.

Distribución: se distribuye o se transmite el malware elegido para el ataque.

Explotación: fase en la que se explota la vulnerabilidad que se ha detectado en el sistema que se está atacando; es el momento en el que el sistema es infectado.

Instalación: momento en el que el malware es instalado en la máquina atacada, si ha de seguir este proceso. No todos los ataques usan esta fase porque a veces pueden robar información sin necesidad de que el malware se instale en el sistema atacado.

Comando y control, C&C o C2 (command and control): en esta fase, el atacante posee el control del sistema atacado y a partir de este momento puede realizar sus acciones.

Acciones sobre los objetivos: el ciberatacante consigue los datos o información que buscaba e intenta extender su ataque a otros objetivos.

Tipos de malware

Los ciberatacantes utilizan el malware con múltiples finalidades: extraer información personal o contraseñas, robar dinero, evitar que un propietario pueda acceder a su dispositivo, etc. Dentro de la utilería base de un ciberatacante, el malware juega un papel protagonista. A continuación, se describen los principales tipos de malware:

Virus: tipo de malware formado por una parte contagiosa de código que infecta otro software en el sistema donde reside y se propaga una vez que se ejecuta.

Gusano (worm): programas que realizan copias de sí mismos, utilizando mecanismos de propagación activos (autoenviándose por correo electrónico) o pasivos (infectando ficheros y esperando a que este sea compartido con otro usuario).

Troyano (trojan): programas que se activan bajo determinadas circunstancias (el primer día de cada mes, después de determinado tiempo de trabajo, etc.) y envían información confidencial del dispositivo a los atacantes o permitiendo que estos puedan acceder al ordenador infectado o incluso controlarlo. Este canal de

exfiltración[3] de información y de control forma parte de una infraestructura C&C.

El troyano SMS (SMS trojan) actúa en un dispositivo móvil haciendo que envíe mensajes SMS (short message service) sin que el propietario tenga conocimiento de ello. Así, sería posible que el usuario se suscribiera a servicios no deseados, enviara correo basura[4] a sus contactos, se autenticara ante entidades bancarias para realizar transacciones, etc.

Ransomware: programas que tienen como objetivo cifrar ficheros o todo el sistema de almacenamiento, informando al usuario de que únicamente mediante el pago de una determinada cantidad de dinero podrá recuperar la información perdida. En general, una vez pagado el rescate (ransom) se recibe la clave de descifrado para recuperar el control y contenido del dispositivo o se elimina el malware correspondiente.

Spyware: malware que recopila y envía información confidencial (identidades, cuentas de acceso, claves, etc.) o cualquier otro dato de tipo personal o empresarial a un servidor externo. En general, los atacantes buscan datos que puedan utilizar más tarde, normalmente con fines económicos. La palabra spyware viene de spy, 'espía', y la aféresis ware de software.

Phisher: los programas de phishing (homófono inglés de fishing: 'pesca') sustituyen las direcciones de páginas de Internet legítimas con otras parecidas pero controladas por los atacantes, de manera que el usuario acaba introduciendo datos confidenciales en la web falsa creyendo que se trata de la original. La forma más extendida de phishing consiste en enviar un correo electrónico suplantando una entidad bancaria (o de otra índole), señalando al usuario que, por diferentes razones, debe conectarse a ese banco y actualizar sus contraseñas. Cuando pincha en el enlace que se le ofrece, en realidad se conecta a otro sitio web, no relacionado con el banco, de modo que cuando teclea sus contraseñas, el atacante las captura, conectándose a la cuenta del usuario y realizando una transferencia bancaria desde la cuenta de la víctima a otra cuenta, propiedad del atacante. Cuando el ataque de phishing no es genérico, sino que va dirigido contra personas, empresas u organizaciones específicas, se conoce como spear phishing. A modo de ejemplo de este tipo de

ataque, podemos mencionar el realizado al servicio web 1&1[5].

Puerta trasera (backdoor): son programas que, utilizando debilidades descubiertas o creadas ex profeso en los sistemas operativos y en las aplicaciones informáticas, permiten el control de dispositivos a través de la recepción de comandos recibidos desde el exterior del dispositivo infectado.

Keylogger: este malware es un programa camuflado en aplicaciones que recoge, guarda y envía a los atacantes la secuencia de teclas pulsadas por los usuarios. Este registrador (logger) de teclas (key) obtiene así información sobre las contraseñas de los servicios a los que el usuario accede desde su dispositivo, los mensajes enviados, etc.

Bot: son programas que ejecutan código de manera automática (bot, aféresis de robot) y remota, con el fin de controlar dicho dispositivo. La red (net) construida por los dispositivos infectados se denomina botnet. En los ataques de denegación de servicio, los ciberatacantes utilizan miles de ordenadores infectados con este tipo de programas para intentar conectarse con la misma página web, lo que provoca que esta página no esté disponible para los usuarios legítimos debido a la elevada carga que soportan durante el tiempo del ataque.

Estafador (scammer): malware cuyo objetivo es engañar y estafar a los usuarios con promociones de viajes o concesión de premios, solicitando dinero para poder acceder a las recompensas anunciadas.

Adware: este malware lleva a cabo falsos clics en anuncios publicitarios sin el consentimiento del propietario del dispositivo, de modo que le muestra publicidad no deseada o engañosa o bien redirige las solicitudes de búsqueda a sitios web de publicidad. El prefijo ad es una apócope de advertising, esto es, ‘publicidad’.

Rootkit: programa que utiliza un kit o conjunto de funciones y métodos no documentados de la interfaz de programación de aplicaciones (API, application programming interface) de un sistema operativo con el objeto de conseguir acceso esencial (root). Un rootkit aprovecha exploits del sistema para conseguir acceso a

nivel deroot y, tras ello, efectuar operaciones de configuración del sistema, así como el despliegue de medidas de ocultación que impidan que sea detectado.

Es importante tener en cuenta que un programa dado puede pertenecer a la vez a varias de estas categorías. Por ejemplo, un programa puede ser un gusano por la forma en que se distribuye, pero a la vez actuar como troyano que se activa en determinadas circunstancias y proporcionar una puerta trasera para que los atacantes puedan tomar el control del equipo. Además, conviene tener presente que en la actualidad existe malware multiplataforma, esto es, que puede ser desplegado en múltiples sistemas operativos.

En paralelo al surgimiento del malware, nacieron multitud de empresas informáticas dedicadas a la detección y eliminación de todo tipo de software malicioso. Comúnmente se considera que el primer antivirus, diseñado en 1972, fue Reaper (‘segadora’ o ‘podadora’), el cual se encargaba de eliminar el virus Creaper (‘enredadera’) en ordenadores DEC PDP-10.

Tabla 1

Principales diferencias entre virus, malware, antivirus y antimalware.

Virus/Antivirus	Malware/Antimalware
Un virus es un tipo específico de malware.	El malware se refiere a todo tipo de softw
Todos los virus son malware.	No todo el malware es un virus.
Un antivirus es un software diseñado para detectar y destruir virus.	Un antimalware es un programa que prot
Los antivirus no pueden proteger el sistema de formas avanzadas de ferrolar	Los antimalware son capaces de defender

Al principio, un programa antivirus se encargaba de la detección de un único virus, pero el aumento del malware propició que algunos profesionales se unieran fundando empresas con los recursos suficientes para realizar un seguimiento de las amenazas y crear antivirus. Algunas de las empresas internacionales que lanzaron sus primeros antivirus fueron McAfee (1987), Symantec (1991) y F-Secure (1991). En el caso de España, las primeras fueron Anyware y Panda Security, que lanzaron sus primeros productos en 1990 (Panda Security, 2020). Además de las anteriores, hoy existen multitud de empresas con productos antimalware como AVG, Kaspersky, McAfee, Trend Micro, G Data, ESET, Avast, Norton, Bitdefender o Virustotal.

Técnicas de malware

Las principales técnicas que siguen los desarrolladores de malware para hacer que este se propague entre los dispositivos de los usuarios son las siguientes:

Exploit: porción de código o programa que aprovecha un fallo de seguridad o una vulnerabilidad en sistemas operativos, aplicaciones o protocolos de comunicaciones para poder realizar cierta actividad. La actividad suele comprometer la seguridad de un sistema o emplearse como parte de los test de intrusión (pentesting), ejecutándose durante la validación de implementaciones de políticas de seguridad[6]. Un tipo especial son los exploitsde día cero (zero-day exploits), que son conocidos por sus desarrolladores y no por el resto de la comunidad informática. Si este tipo de exploit es utilizado por un ciberatacante, se habla de ataque de día cero (zero-day attack), que entraña un serio peligro para los sistemas al no existir mecanismos de detección y control para frenar su avance.

Payload: es la carga útil de un programa de malware, esto es, la

parte del código de un malware que realiza la acción maliciosa. Si el exploitrepresenta una vulnerabilidad, el payloades el código que explota dicha vulnerabilidad. A día de hoy, existen entornos concretos de desarrollo y explotación que dan acceso a repositorios de exploitsy sus correspondientes payloads[7].

Ocultación, enmascaramiento y ataques de evasión: son procedimientos para emular una actividad normal del software y comportarse de forma que no sean detectados por los antivirus/ antimalware o los sistemas de detección de intrusos. Entre otros mecanismos están las técnicas de ofuscación de código[8], desarrollo de aplicaciones nodriza sin payloadpero que descargan dicho payloaduna vez instaladas (como los troyanos de tipo dropper, de dos etapas)[9], procedimientos de mutación del código, o el reempaquetado de aplicaciones del parque de telefonía móvil. El reempaquetado de aplicaciones normales consiste en descompilar una aplicación normal (benigna), gratuita o no, de una tienda de aplicaciones confiable (Play Store de Google, App Store de Apple, Huawei AppGallery, etc.) para insertar en ella el código del mal-ware, luego volver a ensamblar la aplicación troyana y distribuirla a través de una tienda de aplicaciones controlada o no confiable. Estas acciones se suelen realizar mediante herramientas de ingeniería inversa. La técnica se está utilizando con enorme profusión y se considera una gran amenaza para las aplicaciones de dispositivos móviles porque contaminan las aplicaciones normales. Los ingenieros de malware utilizan cada vez más técnicas antiforenses que eliminan de los sistemas todo registro o traza de actividad que puede ser utilizada durante la fase de investigación tras un incidente de seguridad.

Escalada de privilegios: la capacidad de que un malware alcance sus objetivos está limitada por los permisos de acceso a recursos y ejecución de servicios del sistema o dispositivo que está atacando. Para conseguir el mayor nivel de penetración posible, el atacante puede utilizar debilidades en los procedimientos de autenticación y autorización en el sistema objetivo, o puede utilizar un exploitpara aumentar aquellos permisos de acceso y ejecución, consiguiendo, en la situación más crítica, el perfil de administrador de sistema.

Perfiles de atacantes

En ocasiones, los usuarios creen que ni ellos ni la información y datos que almacenan son de la suficiente entidad o no tienen la relevancia necesaria como para ser objeto de ataques. En este sentido, se equivocan, dado que, en muchas ocasiones, no se trata de obtener información particular de un individuo (que también), sino de obtener patrones de comportamiento (lugares donde se viaja, tipo de compras, suscripciones, sitios web que se visita, etc.). Esta información puede agregarse con fuentes abiertas de datos o información extraída desde bases de datos privadas a las que un atacante tiene acceso. El análisis agregado del big data procedente de todas esas fuentes de datos puede emplearse como parte de campañas de publicidad u otras estrategias de empresa (Ríos et al., 2019: cap. 7) como base de conocimiento para construir campañas de phishing y de desinformación y, de forma general, en la fase de extracción de conocimiento de ciberinteligencia en la cyber kill chain.

Por otra parte, es conveniente conocer cuáles son los posibles perfiles de los atacantes, de modo que se tenga una visión de conjunto de a qué se enfrentan los usuarios. Sin embargo, dado que en la actualidad tanto los expertos en ciberseguridad como los ciberatacantes utilizan las mismas o similares herramientas para sus respectivos objetivos, la diferencia entre ambos mundos está más en la intención con las que se usan y en el comportamiento ético de cada uno de ellos. Debido a esto, los profesionales de la ciberseguridad han desarrollado una clasificación de estos expertos según su ética y legalidad. Así, es posible distinguir entre los profesionales de seguridad éticos, los poco éticos y los maliciosos.

De hecho, los hackers de sombrero blanco (white hat) o hackers éticos son los profesionales de la ciberseguridad que siguen un comportamiento ético y se atienen a la legalidad. Su principal objetivo es el de ayudar a mejorar la seguridad de la entidad para la que trabajan. Por otra parte, los hackers maliciosos se clasifican como:

Piratas informáticos de sombrero gris (grey hat hackers): buscan mejorar la seguridad, pero utilizan métodos, técnicas y herramientas que no son éticas, como la piratería no autorizada o la divulgación total de vulnerabilidades, sin dar noticia de ello a los proveedores.

Piratas informáticos de sombrero negro (black hat hackers): su objetivo es estudiar y utilizar técnicas y herramientas de ciberseguridad para obtener ganancias personales a través de actividades maliciosas o de amenazas.

Además, en función de sus intereses se suelen considerar dos tipos de atacantes:

Profesionales: pretenden atacar los tres objetivos de seguridad CID y suelen proceder del mundo empresarial o bien los pagan los gobiernos. Su fin es robar datos confidenciales del público o de empresas con el fin de conseguir beneficios.

Ladrones: utilizan datos o identidades robadas para obtener un ingreso monetario.

Suplantación de usuarios y robos de identidad

Hoy en día, la proliferación de las redes sociales y el uso de Internet en la práctica totalidad de nuestras actividades diarias están asociadas cada vez más con casos de suplantación de identidad. De forma resumida, la suplantación de identidad consiste en hacerse pasar por otra persona para obtener un beneficio, ya sea económico o de cualquier otro tipo (acceso a servicios, reconocimiento personal, comisión de delitos, etc.).

No existe una regulación específica para el delito de la suplantación de identidad dado que el Código Penal regula cada caso de forma diferente en función de la acción que haya llevado a cabo el delincuente. Por ejemplo, en el caso en que se cree un perfil en una red social y se utilice una fotografía de otra persona sin su consentimiento, se trataría de un delito de vulneración de la propia imagen. Si una persona entra en un perfil ajeno y roba contraseñas, se hablaría de un delito de descubrimiento y revelación de secretos. Además, dependiendo del caso específico, también podrían cometerse delitos como los de amenazas, estafa, injurias, calumnias, etc.

Según cifras de la Oficina Europea de Estadística, España es el país de la Unión Europea con más víctimas de ro- bo de identidad registradas: el 7% de los internautas españoles habría sido víctima de este delito en los últimos 12 meses, en comparación con la media comunitaria del 4%. Debido a la facilidad con la que puede crearse un perfil en una red social (en muchas ocasiones, con un correo electrónico es suficiente), los casos de suplantación de identidad se han multiplicado. Con el fin de evitar el aumento de las suplantaciones, algunos servicios ofertados a través de la red han empezado a desplegar procedimientos de registros que exigen usar un segundo medio (como un móvil o teléfono fijo) al que se hará llegar un código de confirmación (a través de un SMS o un mensaje de voz). Además, algunos proveedores también solicitan un

documento identificativo en el que, además del nombre, aparezca una fotografía del usuario (por ejemplo, Uber, Cabify, etc.), lo que supone una primera barrera para aquellas personas que quieran crear un perfil falso.

Esta práctica tiene detractores por cuanto la plataforma que oferta el servicio se hace con información personal, por lo que el usuario debería ser consciente de este hecho y utilizar solo plataformas confiables. En el caso de proveedores de servicio de Internet que usen el pago electrónico o permitan realizar transacciones financieras, existe la obligación de que el registro de usuarios sea robusto para garantizar el correcto enlazado entre la identidad digital y la identidad física del usuario. En concreto, se debe garantizar que dicho proceso sea compatible con procedimientos de tipo "conozca a su cliente" (KYC, know your customer) y con las medidas antiblanqueo de dinero (AML, anti-money laundering) y lucha contra la financiación del terrorismo (CTF, counter terrorism fighting) que la Comisión Europea establece a través de la directiva AML5[10]. Además, en el ecosistema fintech (financal technology, esto es, la industria financiera que aplica nuevas tecnologías a actividades financieras y de inversión), la directiva de servicios de pago (PSD-2, payment services directive) exige que la autenticación se realice de modo robusto[11], lo que involucra la utilización de otros medios para evitar posibles suplantaciones, como son el uso de sistemas de autenticación multimodal, alertas de seguridad cuando alguien se conecta a una red desde un dispositivo que no ha sido dado de alta en la misma, etc.

Formas de suplantación y consecuencias

Entrando en detalle, existen principalmente dos formas de suplantar la identidad de una persona en servicios de Internet:

Acceder ilegalmente a la cuenta: una vez conseguida la contraseña del usuario legítimo mediante phishing o cualquier otro método, el

atacante utiliza el acceso para espiar a la víctima o incluso para hacerse pasar por ella enviando mensajes desde esa cuenta.

Crear un perfil nuevo y falso: utilizando información de la víctima, el atacante crearía un nuevo perfil con la esperanza de que el resto de usuarios crean que se trata del usuario legítimo. Esta situación es especialmente típica en el caso de personas famosas (políticos, deportistas, actores, etc.), donde, en ocasiones, los perfiles verdadero y falso se diferencian en una única letra.

Es responsabilidad de cada proveedor de servicios disponer de un mecanismo por el que las cuentas falsas puedan ser denunciadas por otros usuarios y, en caso de demostrarse el intento de suplantación, desactivarlas. Sin embargo, hay ocasiones en las que, debido a lo común del nombre del usuario legítimo o a que dicho usuario utiliza un identificador no directamente asociado a su nombre (identificador de un puesto de trabajo o un alias), la distancia entre el uso ilegítimo y el derecho al uso de esos identificadores es ciertamente corta, y se pueden realizar desactivaciones de cuentas que no tenían como objetivo la suplantación de identidad. Entre las consecuencias de la suplantación de identidad podemos citar las siguientes:

Compras por Internet: utilizando el número de una tarjeta de crédito, la fecha de caducidad y el número de seguridad, un suplantador podría hacer compras en nombre de otra persona. Debido a ello, algunas tiendas online obligan a pasar un proceso de seguridad adicional.

Aperturas de cuentas corrientes: mediante el uso de los datos de la identidad robada, un atacante podría crear nuevas cuentas corrientes para incriminar a una persona en el futuro o para blanquear dinero en su nombre. En este sentido, es conveniente resaltar la existencia del sistema europeo de reconocimiento de identidades electrónicas (eIDAS, electronic identification, authentication and trust services) establecido en el Reglamento de la UE nº 910/2014, como un conjunto de normas para la

identificación electrónica y los servicios de confianza para transacciones electrónicas en el mercado único europeo. Se introduce aquí el concepto de certificado cualificado en virtud del concepto del proveedor de servicios de confianza (TSP, trust service provider). Esta confianza se basa en la capacidad que tiene un usuario de verificar la validez de un certificado. En el caso particular de que se trate de un sitio web, la verificación se lleva a cabo mediante el certificado de autenticación de sitio web cualificado (QWAC, qualified website authentication certificate), definido en el mismo reglamento.

Robo: al utilizar los datos de la identidad robada, el suplantador podría retirar el dinero de las cuentas bancarias de la víctima o transferirlo a terceras personas para incriminarla en el futuro.

Daño a la reputación: como resultado de algunas de las consecuencias mencionadas anteriormente, es posible que la víctima sea incriminada en actividades ilegales o simplemente reprobatorias (por ejemplo, realizar una donación a un grupo extremista), con el consiguiente daño a su reputación una vez ese hecho sea de conocimiento público.

Desgaste físico y psicológico: recuperar dinero robado por suplantación de la identidad o demostrar que la víctima no es quien realizó las acciones que el suplantador ha realizado en su nombre conlleva un desgaste físico y psicológico. En algunos casos, la dificultad de probar la inocencia de la víctima puede ser tan alta que no consiga hacerlo y su reputación se vea afectada en el futuro.

Buenas prácticas

Tal como se ha comentado, las consecuencias de sufrir una suplantación de identidad pueden llegar a ser muy graves. Debido a ello, es conveniente tener en cuenta los siguientes consejos para que esa situación no llegue a producirse:

No proporcionar información personal confidencial: los datos personales confidenciales (contraseñas, cuentas corrientes, etc.) no deben compartirse ni en persona ni de forma electrónica. Muchos bancos y proveedores de servicios informan, durante el registro de los usuarios, que nunca solicitarán ese tipo de datos por correo electrónico.

No abrir correos electrónicos de usuarios desconocidos: dichos correos pueden contener ficheros ocultos que, al abrirlos el usuario o el programa de gestión de correos, instalen malware en el dispositivo. Incluso en el caso de recibir correos de usuarios conocidos, es importante comprobar que la dirección de correo sea la legítima y que el contenido no despierte sospechas.

Comprobar que las páginas web visitadas sean legítimas: algunos atacantes crean páginas prácticamente iguales a las de los bancos o proveedores de servicios[12], de manera que si la víctima hace clic en la pestaña que se le ofrece o si teclea incorrectamente la dirección de la página web, al final accede a una página fraudulenta que tiene como objetivo obtener sus datos de usuario y contraseña. Para evitar este tipo de problemas, además de asegurarse de visitar solo páginas cuya dirección comience con https:// y muestren un candado cerrado en la barra de estado del navegador, es recomendable instalar un antivirus que compruebe la validez de las direcciones introducidas en el navegador. Por otra parte, cabe mencionar la importancia de actualizar los sistemas de navegación segura. Así, se sabe que el protocolo SSL[13] dejó de estar recomendado por falta de seguridad y en su lugar se recomendó el uso de los protocolos TLS 1.0 y TLS 1.1. Sin embargo, estos dos protocolos han dejado de estar recomendados desde marzo de 2020 y, en su lugar, se recomienda el empleo del protocolo TLS 1.2 y versiones posteriores, lo que aún no se ha puesto en práctica de forma generalizada debido a diferentes causas (entre las que se debe mencionar la pandemia de la COVID-19).

Utilizar contraseñas robustas: contraseñas típicas como la fecha de cumpleaños, el nombre de los hijos o la cadena “123456” son las primeras que prueban los atacantes. Por ello, es importante utilizar contraseñas que mezclen mayúsculas y minúsculas, números y signos de puntuación.

Guardar las contraseñas en un sitio seguro: debido a la cantidad y complejidad de las contraseñas, algunos usuarios pueden verse tentados de escribirlas en un cuaderno o guardarlas en un fichero de texto, sin la debida protección. Proceder de esa manera es, sin embargo, un error, ya que un atacante podría obtener con facilidad esos datos. Para evitar este problema existen multitud de gestores de contraseñas que almacenan esos datos de manera cifrada, de modo que el usuario solo tiene que recordar una contraseña, la maestra (que evidentemente debe ser robusta), para acceder a todas las demás.

Realizar compras seguras: a la hora de realizar compras por Internet, se deben hacer solo en sitios verificados y activar en la tarjeta de crédito la funcionalidad de seguridad que oferta el banco. Además, es altamente recomendable hacer uso de tarjetas prepago (tarjetas monedero) que pueden recargarse con el dinero suficiente para realizar compras online durante un breve periodo de tiempo.

Recopilar pruebas si se sospecha haber sido víctima de una suplantación de identidad (copias de correos, pantallazos de mensajes, etc.) y tramitar la denuncia correspondiente a las autoridades y empresas involucradas.

Denegación de servicio

Los ataques de denegación de servicio (DoS, denial of service) son un tipo de ataque por el que se reduce o anula la capacidad de servidores o recursos informáticos de ofrecer un determinado servicio. Existen diferentes formas de denegación de servicio, como evitar que la página web de una empresa funcione, bloquear el ordenador de un usuario haciendo que el sistema operativo quede inactivo debido a alguna tarea de cálculo intensivo, etc.

La denegación de servicio puede requerir el uso coordinado de cientos (o miles) de atacantes (o equipos de usuarios víctimas de malware) o necesitar únicamente un programa que bloquee el uso del equipo. A continuación, se enumeran los principales tipos de ataques de denegación de servicio:

Saturación: tienen como objetivo acaparar algunos de los recursos críticos del sistema (memoria, almacenamiento, procesador, ancho de banda de las comunicaciones, etc.), provocando su bloqueo. Un ejemplo de este tipo de ataque fue el realizado por un grupo de hackers asociado al colectivo Anonymous en 2010, cuando consiguieron saturar las páginas web de Visa y MasterCard (Addley et al., 2010).

Modificación de la configuración: al cambiar la configuración de elementos críticos de las comunicaciones (routers o servidores de los proveedores de Internet), estos dejan de funcionar adecuadamente, impidiendo que las comunicaciones puedan establecerse. Este fue el ataque al New York Times en 2013, cuando el grupo atacante modificó la configuración que permitía el acceso de los usuarios a las páginas web del periódico (Lee, 2013).

Destrucción de dispositivos: la acción destructiva sobre dispositivos críticos (borrado de partes fundamentales del sistema operativo o

destrucción física del dispositivo) provoca que los servicios atacados no estén disponibles hasta que los equipos afectados hayan sido reemplazados. Un ejemplo fue el ataque, en 2014, a una fábrica de acero alemana que afectó a numerosos sistemas, impidiendo el apagado controlado del alto horno y causando un daño masivo a la infraestructura de la fábrica[14].

Ingeniería social

La ingeniería social consiste en engañar a los usuarios para que faciliten de manera voluntaria información personal confidencial (contraseñas o datos bancarios) que permita el acceso a un equipo e instalar software malicioso. Es una práctica común porque, en ocasiones, es más sencillo engañar a un usuario que vulnerar la seguridad de sus equipos informáticos.

Como ejemplo conviene destacar el llamado fraude o estafa del director ejecutivo (CEO, chief executive officer). En esta estafa, un empleado con capacidad para acceder a datos de las cuentas bancarias recibe un correo, supuestamente de su director, solicitándole ayuda para una operación financiera confidencial y urgente. Si el empleado no se percata del mensaje fraudulento, podría responder al mensaje y caer en la estafa. Este tipo de fraudes se conoce como whaling (caza de ballenas) por tratarse de un phishing dirigido a “peces gordos” (ballena o whale).

En general, en los ataques por ingeniería social se apela a la vanidad, la avaricia, la curiosidad, el altruismo, el temor a las autoridades o incluso nuestros conocimientos informáticos. En cuanto a los elementos utilizados en la práctica, estos pueden ser un correo electrónico, una llamada telefónica o un programa malicioso mediante el que el atacante intente convencer a la víctima para que proporcione sus datos, etc.

Con el fin de evitar ser víctima de la ingeniería social, es recomendable seguir las siguientes instrucciones:

No fiarse de información o noticias recibidas por correo electrónico o en el teléfono móvil, aunque proceda de personas conocidas. En caso de duda, verificar la información por otro canal.

No aceptar ofertas no solicitadas o premios en concursos o sorteos en los que el usuario no haya participado.

No acceder a páginas web cuyos enlaces hayan sido proporcionados por fuentes desconocidas o estén incluidas en otras páginas cuya autoría no se pueda verificar.

No revelar las contraseñas o datos confidenciales nunca, a menos que el usuario sea el que se ha puesto en contacto con la empresa donde se realiza la verificación y se esté seguro de la validez del medio de acceso.

Organizaciones de apoyo a la ciberseguridad

Existen diversas organizaciones que promueven el uso responsable de las redes sociales y otros servicios de Internet y que, de forma habitual, publican información práctica que los usuarios de Internet pueden utilizar para protegerse. A continuación, se describen algunas de estas organizaciones, tanto a nivel nacional (CCN, CNPIC, INCIBE y MCCD) como europeo (ENISA).

El Centro Criptológico Nacional (CCN) es el organismo nacional responsable de garantizar la seguridad de las TIC en las diferentes entidades del sector público y de los sistemas que procesan, almacenan o transmiten información clasificada. Sus funciones están reguladas en el Real Decreto 421/2004, de 12 de marzo. Además, también le afectan otras normas publicadas como la Estrategia Nacional de Ciberseguridad y la Estrategia de Seguridad Nacional[15].

El Centro Nacional para la Protección de Infraestructuras y Ciberseguridad (CNPIC) fue creado en el año 2007 y sus competencias vienen reguladas por la Ley 8/2011. Es el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior.

El Instituto Nacional de Ciberseguridad (INCIBE) trabaja para mejorar el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación, los profesionales, las empresas y, especialmente, los sectores estratégicos. INCIBE, creado en 2006, depende del Ministerio de Asuntos Económicos y Transformación Digital.

El Mando Conjunto de Ciberdefensa (MCCD) fue creado en febrero de 2013 y es el órgano de la estructura operativa, subordinado al jefe de Estado Mayor de la Defensa (JEMAD), responsable del

planeamiento y la ejecución de las acciones relativas a la ciberdefensa en las redes y sistemas de información y telecomunicaciones del Ministerio de Defensa u otras que pudiera tener encomendadas, así como contribuir a la respuesta adecuada en el ciberespacio ante amenazas o agresiones que puedan afectar a la defensa nacional.

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) fue creada en 2004 con el objetivo de contribuir al desarrollo de una cultura de mejora de la privacidad y de la seguridad de la información para el beneficio de los ciudadanos, empresas y organizaciones del sector público de la Unión Europea. En la actualidad, además, tiene como fin proporcionar recomendaciones sobre ciberseguridad, apoyar el desarrollo de políticas y su implementación, y colaborar con equipos operativos en toda Europa.

En los años que lleva en funcionamiento, ENISA ha publicado estudios y recomendaciones útiles para los ciudadanos (Hernández Encinas et al., 2015, 2016). El pasado 2 de julio de 2020 ENISA publicó el esquema de candidatos para la certificación de ciberseguridad (Cybersecurity Certification: EUCC Candidate Scheme)[16]. Se trata de la preparación de un esquema de certificación de ciberseguridad de la Unión como sucesor de los esquemas existentes en el SOG-IS MRA (Senior Officials Group-Information Systems Security Mutual Recognition Agreement)[17]. El esquema pretende analizar la certificación de ciberseguridad de los productos TIC, basada en los criterios comunes (common criteria) establecidos de forma estandarizada para la certificación de productos de seguridad, implantando una metodología común para la evaluación de la seguridad de la tecnología de la información y los estándares correspondientes.

Capítulo 2

Dominios de la ciberseguridad

A lo largo de este capítulo se considerarán los diferentes dominios de la ciberseguridad que afectan a la gestión y procesamiento de la información[18]. Así, se abordarán los aspectos de la ciberseguridad relacionados con los ordenadores personales, los dispositivos móviles, la computación en la nube, el internet de las cosas y las infraestructuras críticas.

Cada uno de los dominios mencionados tiene una serie de rasgos específicos relacionados con las particularidades de computación y gestión de información que llevan a cabo, por lo que las ciberamenazas que pueden afectar a sus activos de información son de muy diversa índole. Dicho de otro modo, no es lo mismo almacenar la información personal en el disco duro de nuestro ordenador personal que hacerlo en un servidor en la nube (Google Drive, Dropbox, etc.). También es muy distinto acceder a la información desde nuestro ordenador conectado a la red corporativa de nuestro despacho que desde un dispositivo móvil conectado a una red pública de un hotel, restaurante o aeropuerto.

Tabla 2

Tipos de activos en los sistemas de gestión de la seguridad de la información.

Activos de información	Activos físicos	Activos de servicios de TI	Activos humanos
Datos digitales: bases de datos, [illegible]	Infraestructura de TI: [illegible]	[illegible] servicios de re	[illegible]
Activos tangibles: correo, fax, llaves, libros, etc.			
Activos intangibles: conocimiento, patentes, etc.	Hardware de TI: estaciones de trabajo, portátiles, etc.	[illegible]	
Software	Controles del entorno de TI: sistema de alimentación inint		
Sistemas operativos			

Fuente: Norma ISO 27001 (https://www.isotools.org/normas/riesgos-y-seg

Ordenador personal

Al comenzar este apartado nos plantearemos algunas preguntas que se habrán hecho muchos usuarios de ordenadores domésticos y a las que trataremos de responder a lo largo de este capítulo: ¿por qué hay tantos ataques contra los ordenadores y dispositivos móviles?, ¿realmente el atacante saca beneficio de los mismos?, ¿compensa tanto esfuerzo o solo son ganas de molestar o de hacerse famoso?

En primer lugar, debemos tener muy presente que en el desarrollo de los ordenadores personales nunca se tuvo en cuenta que hiciera falta protegerlos o dotarlos de seguridad. Se trataba de desarrollar una tecnología que permitiera el uso rápido y eficiente de datos y facilitar la tarea de los profesionales. Baste recordar que los primeros programas que se desarrollaron para el público en general, fuera de los campos militar y de investigación, eran sencillos (vistos a día de hoy) procesadores de texto, bases de datos y hojas de cálculo.

La conexión a una red para compartir información con otros ordenadores llegó mucho más tarde y entonces, salvo en las aplicaciones militares, tampoco necesitaba ser protegida. De hecho, la explosión de las redes tuvo lugar de forma universal cuando la tecnología de la conectividad se empezó a emplear fuera del mundo militar y llegó a las universidades y centros de investigación, donde el principal objetivo era, precisamente, compartir conocimientos con el fin de hacer avanzar los resultados científicos y mejorar la tecnología.

Hoy, cualquier ordenador personal dispone de las suficientes capacidades de almacenamiento y velocidad como para guardar y disfrutar de vídeos familiares, películas, música, además de nuestros datos financieros o médicos. De hecho, como los ordenadores personales contienen tanta información personal y familiar, hemos olvidado que son máquinas muy complejas y potentes, capaces de realizar operaciones que van mucho más allá de lo que requerimos

y que no hace falta tener una profunda preparación previa para usarlas y satisfacer nuestras necesidades. No olvidemos que los fabricantes, a través de sus sofisticados sistemas operativos, hacen que el trabajo con nuestros ordenadores sea no solo amigable, sino hasta "intuitivo".

La mayoría de los usuarios solo "usan" su ordenador y, en general, no saben cómo trabaja ni entienden lo que hay detrás de él. Conceptos como el "registro de Windows" o los "puertos de comunicación" pueden serle desconocidos.

Podríamos ir más lejos si en lugar de hablar del funcionamiento de un ordenador pensamos en los conceptos básicos de seguridad. ¿Cuántos usuarios instalan de forma indiscriminada programas y aplicaciones en sus dispositivos llevados por la publicidad de que las mismas hacen tal o cual cosa o que nos va a hacer la vida más sencilla y cómoda? ¿Cuántas páginas web visitarán, solo porque es fácil hacer clic en un botón, sin haberse interesado previamente (y hasta sospechando) de si el acceso a las mismas es cuestionable?

Los "malos" —como diplomáticamente, y de forma habitual, uno se refiere a los atacantes— son conscientes de que el usuario medio es el eslabón más débil en la cadena de seguridad, por lo que sus ataques se dirigen a quienes le oponen menos resistencia.

Las empresas se han dado cuenta de que muchos de sus empleados mantienen sus prácticas caseras en la oficina, por lo que invierten cada día más dinero y recursos en defender sus activos. A este hecho hay que añadir la explosión del teletrabajo a partir de la pandemia de la COVID-19, que ha puesto de manifiesto la necesidad de establecer unas políticas de seguridad a las que los ciudadanos no están acostumbrados (véanse las conclusiones). De nuevo, los malos buscan el camino más sencillo, que consiste en aprovecharse de las "inocentes" prácticas de los empleados para saltarse estas protecciones y atacar también al mundo empresarial. Así, envían software dañino o malware (véase el capítulo 1) camuflado en archivos adjuntos al correo electrónico, suplantan entidades bancarias, entre otras, y convencen al usuario para que comparta datos de sus tarjetas de crédito, contraseñas o datos personales, siendo entonces víctimas de phishing, etc.

Incluso ahora, a pesar de las numerosas noticias sobre contraseñas y datos comprometidos y sus repercusiones sociales, los usuarios aún quieren compartir sus datos con todos. Las aplicaciones y servicios basadas en Internet, como las redes sociales, hacen que compartir datos sea muy sencillo, basta con hacer clic y ya se ha subido una foto, un vídeo, un fichero a la red y queda a disposición de todo el que desee mirarlo o descargarlo. En resumen, la tendencia de hoy en día es compartir, no proteger. En otro caso, no se entendería esa afición de los usuarios y el crecimiento exponencial en el uso de las redes sociales, en las que sus usuarios desnudan sus datos, gustos, relaciones, vidas, etc. En todo caso, tener una vida social activa no está reñido con la protección de los datos personales y familiares y la privacidad. Es cuestión de equilibrar y conocer los riesgos y amenazas que nos rodean y hasta qué punto restringimos nuestra comodidad de uso por un mínimo de seguridad[19].

Por otra parte, y debido a las características propias de los diferentes sistemas operativos, los ciberataques que se pueden efectuar contra de alguno de ellos, en general, son ineficientes contra los otros. Por este motivo, aunque se puedan describir amenazas o ataques genéricos que afecten de forma similar a cada uno de tales sistemas, la ejecución específica del ataque estará dirigida hacia cada uno de ellos en concreto[20].

A continuación, se presentan algunos aspectos a tener en cuenta con el fin de evitar, o al menos paliar, diferentes tipos de ciberataques que se pueden diseñar y llevar a cabo contra los ordenadores personales, ya sean para uso doméstico o empresarial:

La seguridad es un proceso, no es solo software y hardware: muchas veces se tiene la creencia de que invertir en equipamiento basta para crear una infraestructura segura. Dotar de cortafuegos, sistemas de detección de intrusiones, antivirus, sistemas de cifrado, autenticación fuerte, etc., es bueno y muy conveniente, pero todos estos productos no garantizan por sí mismos la seguridad. Debe tenerse en cuenta que la seguridad es un proceso, esto es, los productos de seguridad solo sirven en la medida en que son correctamente instalados y convenientemente actualizados. De nada sirve cifrar un disco duro para impedir el acceso a los datos que

contiene si las claves empleadas son pequeñas o se han desarrollado nuevas formas de ataque que las hacen vulnerables. Además, también conviene tener bien presente que la seguridad de un sistema viene determinado por la seguridad de su eslabón más débil, lo que obliga a seguir enfoques de tipo integral y a llevar a cabo una monitorización continua de la consecución de objetivos de seguridad.

Amenazas globales: las amenazas basadas en la arquitectura dependen, en general, del modelo empresarial. No es lo mismo atacar a un autónomo que a una pyme o a una gran corporación. También existen amenazas dirigidas contra objetivos específicos. Así, no son igual de frecuentes ni igual de dañinas ni tienen los mismos objetivos las dirigidas contra entidades bancarias que contra una industria farmacéutica. Por último, existen amenazas globales que están dirigidas contra cualquier servicio que tenga acceso a Internet, lo que se puede convertir en la puerta de acceso de un adversario. De hecho, un malware que ataque a una organización en una parte del mundo es muy probable que acabe atacando a otra, en el otro extremo, que posea un software similar.

Gestión de contraseñas: la mayor parte de los dispositivos de red que conectamos a nuestros ordenadores vienen preconfigurados con un nombre de usuario (username) y una contraseña (password). Estos datos suelen, además, aparecer en el manual de configuración del propio dispositivo, por lo que cualquiera puede tener acceso a tal información. De nada sirve una contraseña si está disponible para cualquiera que desee atacar un sistema; así pues, es muy importante cambiar las contraseñas por defecto que traen los dispositivos. Además, cualquier contraseña que se emplee debe ser robusta para impedir que el software diseñado para buscar contraseñas sea efectivo. A esto hay que añadir el hecho de que cada dispositivo debería tener su propia contraseña.

Accesos a la red: dado que las conexiones a la red son habituales y constantes, solemos habilitar dicho acceso de modo automático, sin utilizar contraseñas. La recomendación es no hacerlo así y emplear una contraseña cada vez que realicemos un acceso. Como esta sugerencia rara vez se sigue, sí es muy recomendable, al menos, cerrar los puertos de comunicación que no son necesarios, dado que

un puerto abierto es una puerta que puede dar acceso a nuestro sistema a un atacante. Existen aplicaciones que señalan cuáles son los puertos que se tienen abiertos y la asociación del número de un puerto con su acción puede buscarse en la web.

Actualización del software: la mayor parte de los sistemas operativos y del software tienen la opción de configurarse para que busquen actualizaciones de modo automático. Si no se desea que las actualizaciones se realicen de modo automático porque pudieran dar lugar a incompatibilidades con otro software instalado, la opción de que se notifique la existencia de la actualización, al menos, debería estar activada.

Programas antimalware/antivirus: es muy importante tener instalados programas antimalware y antivirus que protejan los equipos contra todo tipo de software dañino, pero no debe olvidarse su actualización constante, dado que, por ejemplo, nuevas versiones de los virus (mutaciones) pueden sortear esta protección si no se ha actualizado el antivirus correspondiente.

Cuenta de administrador y de usuario: las cuentas de administrador de sistemas se crean para que el mismo tenga acceso a los parámetros de configuración, actualización o cesión de determinados permisos a los usuarios. Este tipo de cuenta solo debería emplearse con estos fines, de modo que si un administrador se conecta para realizar tareas personales, como leer su correo, navegar, etc., debería entrar en su cuenta personal y no como administrador del sistema. Esto es, conviene seguir el principio de mínimo privilegio: hay que contar con el conjunto mínimo de permisos para realizar las operaciones que precisemos en cada momento. Si no se sigue este principio, puede producirse una vulnerabilidad de seguridad, dado que el software malicioso podría ejecutarse con privilegios elevados (eventualmente con permisos de administrador).

Dispositivos móviles

A lo largo de este libro entenderemos que un dispositivo móvil es un dispositivo portátil, esto es, que un usuario puede llevar consigo de forma cómoda y transportar con facilidad (como, por ejemplo, un teléfono inteligente —smartphone— o una tableta —tablet—) y que usualmente tiene menor capacidad de cómputo que un ordenador personal. Sin embargo, no consideramos que tales dispositivos tengan poca capacidad dado que supondremos que todos ellos tienen la posibilidad de conectarse a Internet, realizar comunicaciones a través de la red (correo electrónico, mensajería instantánea, navegación, etc.), realizar fotos de calidad, reproducir música, etc., y con una capacidad de almacenamiento de varios gigabytes.

De forma análoga a lo ya mencionado sobre los sistemas operativos para ordenadores personales, los ataques contra los dispositivos móviles también dependen del sistema operativo que el dispositivo tenga implementado. Los sistemas operativos para móviles más conocidos y extendidos son Android e iOS. Otros sistemas operativos móviles que tuvieron mucha relevancia hace una década fueron Symbian, Windows Phone y BlackBerry.

Según la fuente que se considere, la cuota de mercado de los sistemas operativos varía ligeramente. Así, según Kantar (2020), en Europa y en el último trimestre de 2019, Android tenía 75,0% de cuota e iOS un 24,3%. Con relación a España y en el primer trimestre de 2020, estas cuotas eran del 87,1 y 12,7%, respectivamente. Por su parte, en IDC (2020) se asignó en 2019 una cuota mundial a Android de un 86,1% y a iOS de un 13,9%.

Dos hechos fundamentales que afectan a los teléfonos móviles son que es el medio preferido para el acceso a Internet y que a esta tecnología se han incorporado usuarios de avanzada edad

que tienen un estado poco desarrollado de alfabetismo digital. Esto los convierte en objetivos fáciles para atacantes. Por otra parte, conviene recordar que, en los últimos años, la versatilidad y capacidad de los dispositivos móviles ha crecido de forma sustancial debido al enorme desarrollo y a la facilidad de acceso a la tecnología en la que se basan y a las comunicaciones inalámbricas. Estos dos aspectos han modificado no solo la forma de trabajar de los usuarios, sino la de comunicarse entre sí. Se estima que el número de dispositivos móviles en el mundo en 2020 es de 5.500 millones, esto es, el 70% de la población mundial será usuario de uno[21], por lo que constituirán uno de los principales objetivos para los atacantes, máxime habida cuenta de la escasa atención que sus propietarios dedican a los aspectos relacionados con la seguridad.

Así pues, es importante conocer la seguridad ofertada por estos dispositivos atendiendo a la información que almacenan y gestionan. No olvidemos que en ellos guardamos datos personales (contactos, agenda, fotos, vídeos, mensajes, credenciales bancarias, etc.) e incluso información profesional o corporativa, en algunos casos de interés para la competencia. Además, muchos de estos datos los compartimos en la red, lo que los hace aún más vulnerables y deseables a posibles atacantes.

En definitiva, la primera medida para proteger nuestra privacidad e intimidad (personal y profesional) es ser conscientes de la importancia que tiene la seguridad en tales aparatos móviles y los peligros que puede llevar consigo su mal uso.

El principal enemigo de los dispositivos móviles es el software malicioso o mobile malware, esto es, códigos dañinos, especialmente diseñados para dispositivos móviles, que implementan diferentes ataques y que cada día son más numerosos, complejos y sofisticados.

Por lo general, el malware para móviles suele estar insertado en aplicaciones que los usuarios se descargan e instalan, pero que en realidad ocultan software que actúan en segundo plano y que ponen en riesgo la seguridad del usuario. Algunos de los riesgos que amenazan la seguridad de los usuarios como

resultado de la ejecución de un malware en un dispositivo móvil son (Hamed et al., 2017):

Comprometer la privacidad del usuario robando información confidencial del mismo, bien accediendo físicamente al dispositivo, bien mediante una comunicación establecida con otro dispositivo o servicio o bien a través de una red.

Amenazar la integridad del dispositivo, es decir, tratar de modificar o manipular la información almacenada alterando su exactitud.

Secuestrar los datos del dispositivo, cifrándolos e impidiendo su acceso hasta no haber pagado una determinada cantidad de dinero (ransomware).

Obtener beneficios económicos accediendo a través del dispositivo a las cuentas bancarias del propietario.

Sufrir campañas publicitarias no deseadas o agresivas después de haber visitado webs con información de interés personal.

Utilizar el dispositivo como parte de una botnet, esto es, incluirlo en una red de dispositivos que han sido atacados por un robot (o bot) para realizar acciones maliciosas. Por ejemplo, para ataques por denegación de servicio o DoS (véase el capítulo 1).

Una vez que un atacante ha infectado un dispositivo móvil, este puede afectar a los objetivos de la seguridad (Creutzburg, 2016):

Grabar las conversaciones telefónicas entre el usuario y sus contactos, robar imágenes y vídeos, y enviar información al atacante sin el conocimiento del propietario.

Suplantar la identidad de un usuario para realizar compras en Internet en su nombre o acceder a su cuenta bancaria. Este robo de la identidad puede hacerse a través de la tarjeta SIM del teléfono o

de la información almacenada en el dispositivo.

Eliminar información personal o profesional del dispositivo comprometido.

Hacer llamadas telefónicas no deseadas por el usuario y desde su teléfono, lo que puede generar cargos abusivos para el propietario, o a servicios de emergencia, comprometiendo su disponibilidad y alterando su buen funcionamiento.

Convertir el dispositivo móvil en una máquina zombi, esto es, en una máquina controlada por el atacante desde la que puede enviar mensajes de spam o correo basura, ya sea mediante el servicio de SMS o del correo electrónico.

Inutilizar el dispositivo si el atacante anula su forma de actuar normal o modifica su inicio. Esto se puede conseguir alterando el sistema operativo sin más que borrar o modificar archivos del sistema.

Para paliar los daños señalados existen diferentes listas de recomendaciones básicas que todo usuario debería seguir para mitigar los efectos de tales ataques (INCIBE, 2016; CCN-CERT, 2017b; CCN-CERT, 2018b, 2019b). Se trata, en definitiva, de tener en cuenta una serie de buenas prácticas para evitar, en la medida de lo posible, actos que puedan vulnerar nuestra privacidad y la seguridad de nuestros dispositivos.

Existen varios aspectos a considerar para proteger nuestros móviles, para cada uno de los cuales se incluyen varias recomendaciones. Debe tenerse en cuenta que, en general, la seguridad puede ser inversamente proporcional a la usabilidad, por lo que cada usuario deberá ser quien decida cómo equilibrar ambos aspectos

Proteger el acceso físico no autorizado al dispositivo

Los smartphones son muy deseables por su alto valor económico, por lo que, además de tomar las precauciones normales para impedir su robo, se debe proteger el acceso físico al mismo para evitar que también se sustraigan los datos almacenados en él.

Es necesario establecer un método seguro para acceder al dispositivo, que debe estar bloqueado la mayor parte del tiempo posible (debería bloquearse pasado un minuto, por ejemplo). Existen varias opciones de desbloqueo: PIN (número de identificación personal), patrón gráfico, reconocimiento facial y huella dactilar. Si se opta por el PIN o el patrón, se deberá elegir uno que contenga entre seis y ocho dígitos o puntos de la malla. En el caso del reconocimiento facial, debería probarse que no es posible desbloquear el dispositivo mediante la presentación de una foto del usuario. Si se usa la huella dactilar, sería de gran interés que el dispositivo tuviera algún tipo de sensor que detectara que el sujeto está vivo. Si no se eligen de forma robusta, todos ellos pueden ser vulnerados. De hecho, se sabe que es posible reproducir las huellas de personajes famosos a partir de fotografías de alta calidad mientras hacen el signo de la paz con los dedos, o cuando levantan sus pulgares como signo de acuerdo o aprobación[22].

Recientemente se han comenzado a utilizar dos novedosos sistemas de desbloqueo que no requieren acción alguna por parte del propietario. El primero de ellos es mediante las coordenadas geográficas en las que se encuentra el dispositivo, es decir, es posible activar en el dispositivo la opción de que si este se encuentra en una determinada ubicación (en casa, en el trabajo, etc.), baste con tocar la pantalla para que se desbloquee, sin necesidad de introducir ninguna contraseña o huella. El segundo es mediante la detección de determinados dispositivos en la cercanía del móvil: este está desbloqueado en la presencia de estos dispositivos, como pueden ser los llamados wearables, esto es, los que se llevan puestos, como relojes, pulseras o zapatillas inteligentes.

Minimizar las consecuencias por su pérdida o robo

Es importante realizar con periodicidad una copia de seguridad de los datos almacenados para evitar su pérdida. Esta copia puede almacenarse en un pendrive, en el ordenador personal o en la nube. En este último caso hay que tener en cuenta que puede haber implicaciones no deseables con relación a la seguridad y privacidad de los datos.

Para evitar que algunos extraños puedan acceder a datos confidenciales, es interesante considerar la opción de cifrar el dispositivo. La mayoría de los smartphones incluyen entre sus capacidades la de cifrar el contenido del dispositivo o la de habilitar una parte de su memoria para datos cifrados. Otra opción para proteger nuestra información que está en Internet mediante ese dispositivo que ha sido sustraído consiste en desvincular nuestras cuentas del mismo[23].

Incrementar la seguridad de la información y de los datos almacenados

No es conveniente liberar el terminal (jailbreaking, literalmente 'fuga de la cárcel', en el caso de iOS, o rooting para Android) para acceder a aplicaciones o servicios específicos del sistema operativo, ya que puede comprometer y reducir considerablemente la seguridad del dispositivo.

Al hacer una fotografía, muchos dispositivos móviles incluyen en el fichero correspondiente lo que se conocen como metadatos: fecha y hora de su creación, modelo del dispositivo, tiempo de exposición de la foto, apertura, distancia focal, etc., siguiendo el estándar EXIF (exchangeable image file format). También ofrecen la posibilidad de añadir las coordenadas del sistema de posicionamiento global (GPS, global positioning system). Por ello, es conveniente desactivar esta opción o bien restringir el número de personas con las que se comparten tales imágenes para evitar brechas de privacidad[24].

Proteger las comunicaciones que se realicen con otros equipos y servicios

No es conveniente conectarse mediante redes públicas no confiables (bares, restaurantes, hoteles, aeropuertos, etc.) si se van a transmitir datos confidenciales o personales. Para asegurarlos, existen aplicaciones que los cifran, como las redes privadas virtuales (VPN, virtual private network).

Debe prestarse atención a la publicación de información personal o de imágenes en las redes sociales (Facebook, Twitter, Instagram, etc.), dado que puede ponerse en riesgo la privacidad de otras personas, no solo la propia. La información colgada en estas redes es susceptible de emplearse para chantajear o coaccionar a las personas relacionadas con la misma.

Además, es conveniente activar el acceso mediante PIN a las conexiones bluetooth y NFC (comunicación de campo cercano) y configurar el dispositivo en modo oculto. No se deben aceptar conexiones de dispositivos que no sean conocidos (CCN-CERT, 2018a).

También, se debe desactivar la previsualización de los mensajes (correo, SMS, etc.) y adjuntos, y borrar los de origen desconocido. También es importante desactivar el redireccionamiento directo de los códigos de barras (tipo QR, de respuesta rápida) a páginas web para revisarlas con antelación.

No conectar el dispositivo a puertos de serie universal o USB que no sean de confianza. Este puerto permite no solo cargar la batería, sino también establecer conexiones a otros equipos. El ataque juice jacking consiste en extraer datos personales o ejecutar acciones dañinas, a través del puerto USB, cuando se supone que se está cargando el dispositivo. Siempre que se pueda, es conveniente configurar el dispositivo en modo "solo

carga" para evitar compartir datos o ficheros. También existen conectores (preservativos USB) que, colocados entre el dispositivo y la toma de alimentación, solo permiten la carga y bloquean la transferencia de datos.

Actualizar y configurar adecuadamente las aplicaciones instaladas

Es muy importante mantener actualizado tanto el sistema operativo del dispositivo móvil como las aplicaciones instaladas. De este modo se reducirán considerablemente las posibles vulnerabilidades que se hayan detectado. En general, se recomienda instalar solo las aplicaciones de tiendas oficiales (Google Play, App Store, etc.) y no descargar e instalar software de lugares no confiables.

Es conveniente revisar la configuración por defecto del dispositivo dado que, en numerosas ocasiones, la mayoría de los servicios están activados para poder hacer un uso inmediato de los mismos. Así, es recomendable desactivar los servicios que no son de uso cotidiano o considerados críticos.

Es recomendable leer las valoraciones y comentarios de otros usuarios antes de instalar una aplicación a fin de conocer las opiniones de quienes ya la han usado con antelación. Además, es importante revisar los permisos que tales aplicaciones solicitan no sea que resulten excesivos. A modo de ejemplo, si un usuario desea instalarse una lupa o una linterna, no debería consentir que tal aplicación pidiera permiso para acceder a sus contactos o a la agenda.

Computación en la nube

La computación en la nube (cloud computing) es una tecnología de sistemas informáticos que determinados proveedores de servicio (CSP, cloud service provider) ofrecen a los usuarios y empresas de modo que puedan disponer de sistemas de almacenamiento masivo, obtener y compartir información, comunicarse, jugar, etc. (Hamed et al., 2017). Estos servicios se ofrecen, en general, mediante máquinas virtuales (VM, virtual machine) de modo gratuito o mediante un pago por el servicio.

La nube representa un modelo de computación y tratamiento de la información que aumenta la productividad. Ahora bien, esto supone depender de los medios y recursos de computación de un tercero, el proveedor de servicios.

La tecnología de la nube tiene dos características: virtualización y multitenencia. La virtualización permite compartir recursos hardware con el objetivo de ejecutar computaciones para las que un usuario o empresa no posee capacidad, lo cual facilita el ahorro de costes al no tener que invertir en infraestructuras. Por otra parte, la multitenencia posibilita que los usuarios almacenen y traten sus datos a través de las aplicaciones ofrecidas por el CSP y que son compartidas con otros usuarios.

En definitiva, la computación en la nube es una tecnología que maximiza la capacidad de computación minimizando costes. Abordar este tema para el mundo empresarial sobrepasa los objetivos de este libro por lo que nos restringiremos a los principales aspectos de la tecnología y de seguridad más destacados para los usuarios. Así, presentaremos brevemente los diferentes modelos de computación en la nube, sus riesgos, las técnicas de intrusiones en los servidores de la nube y algunos de los tipos de ataque más importantes[25].

Tipos y modelos

En función de quien sea el titular de la infraestructura en la nube, se suelen considerar cuatro tipos de infraestructuras:

Pública: en este tipo de nube se encuadran aquellas para las que la infraestructura y los recursos lógicos ofertados están disponibles para el público en general.

Privada: es propiedad de la empresa que lo implanta con sus propios recursos.

Comunitaria: es la nube creada por dos o más empresas para implementar una infraestructura con unos objetivos y un entorno común para los temas de seguridad y privacidad.

Híbrida: este tipo de nube se presenta cuando se unen dos o más de los tipos anteriores.

Por otra parte, los modelos de computación en la nube se han construido atendiendo al tipo de servicio que se ofrece, por ello, en general, se consideran tres modelos diferentes:

Software como servicio (SaaS, software-as-a-service): en este caso el CSP suministra el software para el usuario de modo que este se ejecuta en la infraestructura de la nube (red, servidores, sistemas operativos, etc.). Por esta razón, el consumidor del servicio no tiene ninguna responsabilidad en la administración o el mantenimiento de dicha infraestructura. Un ejemplo de SaaS es Google Maps.

Plataforma como servicio (PaaS, platform-as-a-service): el proveedor proporciona una plataforma al consumidor para que este

implemente sus propias aplicaciones. Tampoco en este caso el consumidor es responsable de mantener la infraestructura, pero sí controla las aplicaciones implementadas y la configuración de su alojamiento. Google App Engine y Microsoft Azure son ejemplos de PaaS.

Infraestructura como servicio (IaaS, infrastructure-as-a-service): en este modelo, el CSP ofrece al consumidor el procesamiento, almacenamiento, redes y cuantos recursos informáticos necesite el consumidor para que este pueda ejecutar su software. En este caso, la gestión de la infraestructura corre a cargo del CSP. Ejemplos de IaaS son Amazon Web Services[26] y Eucalyptus.

Estos tres niveles de abstracción responden al modelo de servicios en la nube del NIST (2011b), de modo que el gradiente IaaS-PaaS-SaaS representa un incremento gradual en el nivel de confianza del usuario respecto al CSP.

Tabla 3

Esquema de los modelos en la nube y su gestión.

Servidor	Software propio	Plataforma como servicio (PaaS)	Software como servicio (SaaS)
Gestionado por el cliente	Aplicaciones	Aplicaciones	Aplicaciones
Datos	Datos	Datos	Datos
Tiempo de ejecución	Tiempo de ejecución	Tiempo de ejecución	Tiempo de ejecución
Middleware	Middleware	Gestionado por el CSP	Middleware
Sistema operativo	Sistema operativo	Sistema operativo	Sistema operativo
Virtualización	Virtualización	Gestionado por el CSP	Virtualización
Servidores	Servidores	Servidores	Servidores
Almacenamiento	Almacenamiento	Almacenamiento	Almacenamiento
Interconexión	Interconexión	Interconexión	Interconexión

En la actualidad existe una tendencia cada vez más arraigada de diseñar y desplegar arquitecturas software que no cuenten con un servidor, sino que hagan uso de los servicios disponibles a través de las API de uno o varios CSP. A este tipo de esquemas se los llama serverless. En ocasiones no es necesario tener acceso continuo a los servicios cloud, sino que basta con ejecutar tales servicios en un momento concreto y durante un espacio de tiempo limitado. En este esquema de operación se habla de la ejecución de microservicios y se hace uso de una nueva tecnología de virtualización, la contenerización, o bien se incluye una nueva capa de servicios: la funcionalidad como servicio (FaaS, function-as-a-service). En el caso de que se opte por emplear microservicios mediante contenerización, se virtualiza la funcionalidad concreta de un sistema operativo en lugar de virtualizar el sistema operativo completo. Esto genera un vector nuevo de multitenencia, que tendrá sus repercusiones en términos funcionales y de seguridad.

Riesgos y amenazas

La seguridad en la nube viene dada por el conjunto de técnicas, protocolos y controles que proporcionan protección a las aplicaciones, los datos y la infraestructura alojada en la misma. Dado que la proliferación de estos servicios es cada vez mayor, el número de ataques diseñados contra los mismos ha crecido en la misma medida. De hecho, el que los usuarios suban su información a la nube puede exponerlos a diferentes riesgos (Hamed et al., 2017; INCIBE, 2011):

Comprometer la privacidad o robar información sensible: cuando los usuarios suben su información a la nube dan por hecho que nadie accederá a la misma sin su consentimiento. Sin embargo, esto no siempre es así y se corre el riesgo de que los atacantes puedan robar las credenciales de un usuario y acceder a sus datos, lo que

comprometería la CID de estos servicios[27].

Denegación de servicio (DoS): se produce cuando el atacante es capaz de enviar un número tan grande de solicitudes para acceder a la nube que los servidores no pueden dar abasto y colapsan el sistema de modo que los usuarios no pueden acceder a los servicios (véase el capítulo 1).

Pérdida de datos: si el CSP es víctima de un ataque por el que llega a perder datos, es posible que pierda la confianza de los usuarios, quienes dejarán de contratar sus servicios[28].

Acciones de empleados (insiders) maliciosos: en este caso, son los que están dentro de la organización o empresa con capacidad de decisión y acción (insider) quienes pueden llevar a cabo actos contra los usuarios aprovechando sus permisos de acceso. Con ello pueden lograr el desprestigio de la empresa y sus consiguientes pérdidas financieras.

Interfaces de programación inseguras: en general, los CSP ofrecen una serie de interfaces o API para que los desarrolladores de software y los usuarios interactúen con los servicios y aplicaciones de la nube. Como los procesos de autenticación, autorización, etc., se llevan a cabo mediante estas API, es importante que las mismas estén desarrolladas e implementadas de forma segura.

Desconocimiento de la tecnología cloud por parte del usuario final: el desconocimiento de la infraestructura subyacente a la cloud empleada puede suponer un riesgo. Por ello, es importante tener información sobre la tecnología de la plataforma: con quién se comparten los datos, los intentos de acceso no autorizados que se han producido, el país en el que está implementada la nube y su legislación correspondiente, etc.

Fuentes de intrusiones

Existen varias fuentes que pueden dar lugar a intrusiones en los

sistemas de computación en la nube:

Ataques desde fuera de la nube: un atacante podría tratar de enviar una enorme cantidad de solicitudes para acceder a la máquina virtual de la nube, produciendo el fallo del servicio de esta para los usuarios legítimos (ataque DoS).

Ataques desde una red virtual: en este caso, los atacantes son capaces de explotar algunas vulnerabilidades del sistema y comprometer las máquinas virtuales, de modo que lanzan un ataque distribuido de denegación de servicio (DDoS, distributed DoS).

Ataques desde un hipervisor malicioso: un hipervisor (o monitor de máquina virtual) es un software responsable de administrar el intercambio de una plataforma de hardware entre diferentes sistemas (virtualización). En general, los hipervisores no son códigos muy extensos y su comunicación con la parte externa es limitada.

Técnicas de intrusiones

Las principales técnicas empleadas por los atacantes para lograr intrusiones en los sistemas de computación en la nube son las de reconocimiento, de denegación de servicio y de inyección de malware.

Las técnicas de reconocimiento están generalmente relacionadas con el pirateo y se llevan a cabo recopilando la mayor cantidad de información posible sobre la víctima. Algunas de estas técnicas son:

Ingeniería social: utilizar las normas sociales o los sentimientos individuales para obtener información sensible.

Bucear en el basurero: obtener información confidencial de las

papeleras (basura).

Herramientas de Usenet (red de usuarios): obtener información y datos de posible interés a partir de los sitios web de la empresa y de la información que los empleados de la misma suben a las redes sociales, entre otras.

Explotación de la primitiva de transferencia de zona en un servidor DNS: recabar información relevante de un servidor de sistema de nombres de dominio (DNS, domain name system)[29], como, por ejemplo, la dirección de un servidor de correo, de un servidor web, etc. Una mala configuración del servidor DNS de una organización puede hacer posible que un atacante enumere todos los dominios registrados dentro de la red de dicha organización.

Las técnicas de denegación de servicio son fáciles de implementar, pero es difícil protegerse contra ellas. De hecho, el ataque consiste en consumir determinados recursos del sistema de computación en la nube, como el ancho de banda de la red, la memoria o el espacio de almacenamiento, mediante el envío de una gran cantidad de solicitudes de acceso que son ilegítimas y cuyo número es superior al límite que el sistema puede atender, de modo que los usuarios legítimos ven su acceso al sistema denegado (DoS y DDoS). El tipo más común de este ataque es el DDoS, esto es, el ataque DoS distribuido que utiliza miles de ordenadores para lanzar el ataque.

Los atacantes también pueden utilizar determinadas herramientas para lograr el descifrado de las cuentas obteniendo sus contraseñas. El atacante puede usar esas herramientas para descifrar un archivo de contraseña de hashes. Dicho de otro modo, las contraseñas no se almacenan en claro, sino que en su lugar se almacenan unos resúmenes suyos (calculados mediante unas funciones llamadas hash), de modo que lo que el atacante intenta, al acceder a la nube, es hacerse con el fichero que almacena los hashes de las contraseñas e intentar recuperar las mismas para luego descifrar el contenido de las cuentas.

Algunas de las técnicas más utilizadas para obtener las contraseñas son las siguientes:

Ataque por fuerza bruta: el atacante prueba todas las posibles combinaciones de caracteres hasta localizar la que corresponde a la contraseña buscada.

Ataque por diccionario: se trata de utilizar una colección de palabras (diccionario) que los usuarios emplean habitualmente como contraseñas, hasta localizar la que corresponde a la víctima.

Ataque híbrido: es el que combina los dos ataques anteriores.

Al igual que ocurre con las aplicaciones web, y de modo muy resumido, las aplicaciones cloud responden a un modelo cliente-servidor en el que cabe diferenciar la sección del servidor (backend) de la interfaz del usuario (frontend), así como el módulo de persistencia de información, que suele implementarse mediante una base de datos. La programación de cada una de esas secciones responde a una lógica distinta y hasta a un lenguaje de programación diferente. La ejecución de cualquier aplicación, al margen de que el backend esté o no en la nube, requiere la transferencia de información entre esos tres elementos. Dicha transferencia exige la interpretación de la lógica del módulo de origen en términos de la lógica del módulo de destino. Esa conversión suele ser problemática y, en caso de que no se realice de modo correcto, puede habilitar ataques, entre los que destacan:

La técnica de inyección de lenguaje de consulta estructurado (SQL, structured query language) consiste en utilizar este tipo de lenguaje para realizar consultas concatenadas a los servidores de bases de datos del CSP. Los atacantes pueden explotar estas vulnerabilidades para inyectar scripts (programas simples o secuencias de comandos que interactúan con el sistema operativo) maliciosos de modo que puedan obtener el acceso no autorizado a las bases de datos.

El ataque XSS (cross-site scripting) se considera hoy en día una de las técnicas de ataque más dañinas y peligrosas en el dominio de las

aplicaciones web en general, y en particular en el caso de aplicaciones web móviles desplegadas en la nube. Se llevan a cabo inyectando scripts maliciosos (JavaScript, ActiveX, HTML, etc.) en una página web vulnerable para que tales scripts se ejecuten en el navegador web de la víctima.

Tipos de ataque

Al igual que en otros ámbitos contenidos en este capítulo, la computación en la nube ha visto incrementados los tipos de ataques contra su actividad y servicios debido a su uso cada vez más frecuente. Tales ataques se pueden dirigir contra diferentes elementos de la nube: redes, información, estructura, etc.

Falsificación del protocolo de resolución de direcciones (ARP)

Este ataque modifica el flujo de los datos enviados desde el ordenador (la víctima) para hacer un ataque de tipo hombre-en-el medio (MitM, man-in-the-middle), logrando que el tráfico de la víctima pase por la máquina atacante, sin que ello sea apreciado por la víctima, antes de llegar a la puerta de acceso (gateway) de su destino. El atacante debe estar en la misma red local (LAN, local area network) que la víctima y, entonces, se colocará en medio del tráfico pudiendo examinar todo lo que se transmite entre la víctima y el gateway.

La clave para el éxito de este ataque está en aprovechar la configuración por defecto del protocolo de resolución de direcciones (ARP, address resolution protocol). En efecto, cuando se quiere entregar un paquete IP a alguien dentro de una LAN, la entrega no se hace mediante su dirección IP, sino de su dirección MAC[30] (media access control). Eso significa que hay que traducir la dirección IP a la dirección MAC, lo que se puede llevar a cabo a través del ARP, que hace corresponder una IP con su correspondiente MAC. Las entradas de la tabla de

enrutamiento se van añadiendo a medida que los paquetes viajan por la LAN. Es entonces cuando el atacante engaña a la víctima y al gateway, haciéndoles creer que él es el extremo adecuado de la comunicación:

Ataques DoS y DDoS: estos ataques ya han sido comentados anteriormente y tienen como objetivo evitar que los usuarios legítimos accedan a los recursos de la red.

Suplantación de identidad de protocolo de Internet: este tipo de ataque suele emplearse también en los ataques DDoS pues oculta la identidad del atacante. El hecho de ocultar la identidad de las máquinas participantes ayuda al atacante a no ser rastreado y a engañar al CSP.

Escaneo de puertos: este ataque busca en los servicios de red disponibles intentando explotar los canales de comunicación para lanzar un ataque posterior. Una de las formas de escaneo más empleadas es la de conexión de puertos del protocolo de control de transmisión (TCP, transmission control protocol).

Hombre en la nube: se trata de un ataque bastante popular que se dirige a aplicaciones de almacenamiento (Dropbox, Google Drive, etc.). Se basa en la explotación de los protocolos de sincronización y las aplicaciones de autenticación del usuario. El ataque supone el acceso a una cuenta de la víctima utilizando sus credenciales de autenticación, sin la necesidad de descifrar la contraseña.

Ataques internos: en este caso, el ataque proviene de un usuario autorizado en el lado del proveedor con el fin de obtener privilegios para realizar una actividad maliciosa contra los usuarios o el CSP.

Internet de las cosas

El internet de las cosas hace referencia a todo tipo de redes que incluyen objetos, artefactos, electrodomésticos, atuendos, implantes médicos, etc., que llevan incorporados componentes electrónicos, software y sensores que les permite recoger información en tiempo real para tener una contextualización de su situación y, de ser necesario, comunicarla convenientemente (CCN-CERT, 2017a).

Estas "cosas" son capaces de entenderse entre sí y no necesitan de una interfaz para manejar los datos que recopilan. No obstante, en ocasiones necesitamos que estas cosas nos muestren parte de su información, para lo que recurrimos a visualizar estos resultados o notificaciones mediante interfaces y pantallas. Aquí intervienen los aspectos relacionados con el hardware y software de la IoT.

Uno de los principales problemas en ciberseguridad es que estos artefactos de uso común ya no están aislados, sino que pueden estar conectados a otros dispositivos que podrían acabar por convertirse en ejércitos de botnets con el fin de realizar acciones maliciosas.

Un notable ejemplo de este tipo de ataques es el ataque debido al malware Mirai[31], que podía hacerse con el control de dispositivos IoT con poca seguridad como cámaras de seguridad, grabadoras de vídeo digital y enrutadores para usarlos en ataques en línea a gran escala.

A continuación, se tratarán diferentes aspectos relacionados con la IoT, como sus elementos, los riesgos que entraña su uso, los diferentes tipos de ataque que puede sufrir (Patil et al., 2017; Stallings, 2017) y una serie de recomendaciones a modo de buenas prácticas (CCN-IoT, 2017).

Elementos de la IoT

En ocasiones se considera que la IoT no es tanto una red de cosas físicas como una red de dispositivos que interactúan con cosas físicas y con plataformas de aplicaciones como ordenadores, tabletas y smartphones (Stallings, 2017). Así, algunas publicaciones se suelen centrar en dos de los elementos de la IoT: las cosas que están conectadas y la red (Internet) que las interconecta. No obstante, con el fin de dar una visión más amplia de los elementos que forman parte de la IoT, consideraremos los siguientes:

Los sensores y actuadores son las cosas de la IoT. Los sensores observan su entorno, esto es, recopilan información para contextualizar su situación e informan de las mediciones realizadas de diferentes variables (temperatura, humedad, etc.). Por su parte, los actuadores operan en su entorno de modo que cambian la configuración de un sensor o hacen operar determinados componentes que contienen o que están cercanos (termostato, etc.).

La conectividad permite a un dispositivo conectarse a una red (inalámbrica o por cable) para enviar los datos que ha recopilado al centro de datos (sensor) o para recibir comandos operativos del controlador (actuador).

La red que admite los dispositivos debe tener la capacidad de manejar el flujo de datos requerido, en general, bastante elevado.

La instalación debe tener una alta capacidad de almacenamiento para guardar la información recogida y para mantener las copias de seguridad de todos los datos recopilados.

Se debe disponer de capacidad para el análisis de datos. Téngase en cuenta que cuando se dispone de muchos dispositivos, se genera big data, lo que precisa de mucha capacidad de análisis para procesar el flujo de información.

Tipos de dispositivos

Con relación a los dispositivos de la IoT, se suelen distinguir entre los de transporte de datos (data-carrying devices) como las etiquetas de identificación por radiofrecuencia (RFID, radio frequency identification) y los portadores de datos (data carriers), como los elementos adjuntos a una cosa física con el propósito de identificarla y proporcionar algún otro tipo de información. Las tecnologías utilizadas para la interacción entre los dispositivos de captura de datos y los dispositivos que transportan datos o los portadores de datos incluyen radiofrecuencia (etiquetas), infrarrojos (control remoto), óptica (códigos de barras) y conducción galvánica (dispositivos médicos implantables).

Atendiendo a los diferentes usos de los dispositivos IoT, conviene recordar algunos de los más empleados:

Smart home (hogar inteligente): las casas u hogares inteligentes pueden ser una de las aplicaciones de mayor éxito en la IoT. Ya no es extraño encontrar aplicaciones móviles que avisan de posibles intrusiones en el domicilio, conectan determinados electrodomésticos o la calefacción, etc. También es posible controlar otros aspectos de la casa, como la iluminación, música, etc., mediante la voz o a través de los altavoces inteligentes (Alexa de Amazon, Google Home, Apple HomePod, etc.).

Wearables (tecnología vestible): se llaman así a los pequeños dispositivos como pulseras deportivas (smart bracelet) o relojes inteligentes equipados con sensores capaces de medir determinadas variables corporales (tensión, ritmo cardiaco, número de pasos, etc.) e informar sobre las mismas a sus portadores con el fin de organizar determinadas actividades personales, como consumo de calorías, rendimiento deportivo, etc. También las gafas virtuales (smart glasses) dotan de determinadas capacidades para extender los sentidos, de forma que su uso puede convertirse en soporte y despliegue de funcionalidades y aplicaciones de realidad aumentada.

Smart city (ciudad o espacio inteligente): este nuevo concepto hace referencia al uso de numerosos tipos de sensores (contadores inteligentes de luz o agua) para hacer más fácil, segura y eficiente la vida en las

ciudades o sus espacios[32]. Estos dispositivos están conectados a Internet, recopilan, procesan y analizan los datos que ayudan a las centrales correspondientes a tomar decisiones sobre los usos de los consumidores, detectan fallos en el suministro, etc. A la vez, pueden informar a los usuarios de su consumo y hasta recibir alertas en caso de uso excesivo o fugas. Otros sensores pueden ayudar a gestionar el tráfico, detectar zonas de alta contaminación ambiental, aumentar la seguridad ciudadana, etc. En todo caso, el despliegue de estos contadores inteligentes no está exento de polémica por motivos de seguridad (Chamareta et al., 2020)[33].

Logística y mantenimiento industrial: el control en el envío de paquetes en un determinado plazo de tiempo, el seguimiento en tiempo real de su localización, la gestión eficiente de los vehículos de transporte, etc., son temas importantes en la logística de una empresa. También el mantenimiento industrial se ve favorecido por la combinación de sensores y software especializado que permite una disminución de costes y, consecuentemente, un aumento en los beneficios. La llamada industria 4.0 se beneficia de la IoT por el uso más eficiente del almacenamiento de mercancías y el procesamiento de datos.

Vehículos y drones: la IoT está presente en vehículos, tripulados o no. Cada día son más frecuentes las aplicaciones que indican los trayectos más convenientes para viajar en tiempo real (Google Maps, TomTom, Sygic, etc.), o el uso de sensores de movimiento, proximidad y cámaras para el autoestacionamiento. Otros sensores en los vehículos permiten conectarlos a Internet, a través de las llamadas redes vehiculares ad hoc (VANET, vehicular ad-hoc network), de modo que pueden recopilar información útil para el conductor a lo largo de su viaje, o el reciente desarrollo de los vehículos autónomos. El uso de drones para el control de incendios, reparto de mercancías, vigilancia, entorno militar, etc., es otro de los aspectos más novedosos dentro de este campo.

Salud: el empleo de los dispositivos médicos implantables (IMD, implantable medical device) ha supuesto una revolución en el mundo de la medicina y la salud de los ciudadanos (FDA, 2020; Ferguson et al., 2011). Entre estos dispositivos destacan marcapasos, bombas de insulina o morfina, dispositivos

anticonceptivos subcutáneos, etc. Es importante señalar la importancia del control preciso y exhaustivo de la seguridad de los IMD porque pueden afectar a la calidad de vida o al desarrollo de una enfermedad del portador. No solo es posible vulnerar la privacidad de los pacientes implantados al acceder a los datos que los IMD suministran, sino que un ataque activo podría modificar las condiciones de funcionamiento de dicho implante y derivar catastróficas consecuencias para el paciente[34]. Otros usos de la IoT en el mundo sanitario son la teleasistencia y la ayuda al diagnóstico no presencial, así como la integración de esta tecnología en las camas de hospital que, equipadas con sensores especiales, permiten observar determinados valores de los pacientes (presión sanguínea, volumen de oxígeno, temperatura corporal, etc.).

Agricultura y ganadería: hoy en día, las granjas inteligentes son una realidad. De hecho, los agricultores se benefician al poder predecir y cuantificar cada cosecha antes de recogerla debido a la información detallada que determinados sensores pueden ofrecer acerca de las condiciones del suelo: humedad, acidez, temperatura, características químicas, condiciones de riego, presencia de enfermedades, etc. También la ganadería obtiene ventajas de la IoT al emplear, por ejemplo, chips biométricos para el seguimiento y geolocalización de los animales.

Hostelería: algunos restaurantes, sobre todo de comida rápida, tienen terminales en los que se elige y paga la comida y posteriormente avisan de cuándo esta está lista para recogerse. También las llaves electrónicas en algunos hoteles se envían a los móviles de los huéspedes, con lo que se automatizan determinadas tareas, como la apertura de puertas, peticiones al servicio de habitaciones, pequeñas compras, etc. También aquí se han producido determinados ataques[35].

Riesgos y amenazas

Los riesgos y amenazas de la IoT pueden aparecer a lo largo de cualquiera de los procesos que intervienen en la misma: captura de

datos, almacenamiento, transferencia, agregación y procesado, así como en la provisión de los servicios que involucran a la IoT (NIST, 2019; UIT, 2018). A continuación, se detallan los posibles riesgos y amenazas:

Comprometer la seguridad en las comunicaciones y en la gestión de los datos: para evitar este riesgo es importante que las comunicaciones que se establezcan entre las partes y la gestión de los datos sean seguras, confiables y garanticen su privacidad.

Comprometer la seguridad de la provisión del servicio: es preciso que la provisión de servicios sea segura, confiable y proteja la privacidad. De este modo se garantiza que no se producirán accesos no autorizados al servicio y no se proporcionará tal servicio de forma fraudulenta.

Falta de integración de políticas y técnicas de seguridad: es necesaria una adecuada capacidad para integrar las diferentes políticas y las técnicas de seguridad. De esta manera se garantizará un control de seguridad que sea consistente con la variedad de dispositivos y redes de usuarios en la IoT desplegada.

Defectos en la autenticación y autorización mutuas: con el fin de evitar accesos no deseados, antes de que un dispositivo (o usuario) pueda acceder a la IoT, es preciso garantizar que la autenticación y la autorización mutua entre el dispositivo (o usuario) y la IoT se realizan conforme a las políticas de seguridad establecidas de antemano.

Defectos en la auditoría de seguridad: si la auditoría de seguridad de la IoT no es compatible con las regulaciones y normas establecidas, pudiera suceder que los accesos a los datos o a las aplicaciones de la IoT no fueran totalmente transparentes, rastreables y reproducibles.

Tipos de ataque

Los diferentes tipos de ataque se clasifican en los que afectan a la privacidad, al control y a la disponibilidad. A continuación se detallan aspectos más concretos de ataques:

Ataque a la privacidad

Reconocimiento: hace referencia al sondeo inteligente para acceder a las vulnerabilidades en una red, con el fin de lanzar un ataque a gran escala más adelante.

Escuchas (eavesdropping): consiste en estar al tanto de las comunicaciones con el fin de conocer los datos agregados que están siendo recopilados por toda la red. Las escuchas entre dos nodos[36] de sensores específicos no siempre suponen una ayuda para el atacante.

Ataque al control

Hombre en el medio (MitM): en este caso, el atacante intenta establecer una conexión entre un conjunto de nodos y el nodo central (o sumidero), de modo que los nodos en la red no se percatan de que el atacante es capaz de manipular el control del flujo de información.

Interferencia por radio: dado el creciente número de tecnologías inalámbricas que utilizan el mismo espectro de banda (2,4 GHz, 5 GHz o 900 MHz), es posible montar ataques provocando interferencias de radio. Así, en un entorno urbano, donde los smartphones comparten el mismo espectro, se puede producir una degradación del rendimiento de los nodos individuales debido a la interferencia de radio. El mismo ataque se puede establecer en redes de sensores si se incrementa considerablemente el número de

nodos de sensores.

Inyección: si un atacante es capaz de acceder a una red, podría hacerse con alguno de los nodos del sensor e inyectar datos o software maliciosos en la red. Estos datos maliciosos podrían ser falsos anuncios de información entre nodos vecinos, lo que podría conducir a suplantar nodos sumideros.

Repetición: un atacante podría interceptar datos de un usuario y retransmitirlos posteriormente. El ataque es efectivo durante los procesos de distribución de claves compartidas o contra los esquemas de autenticación que sean débiles o que no empleen marcas de tiempo cuando se autentican los nodos.

Bizantino: es un tipo de ataque interno en que el atacante se hace con el control de varios nodos de una red y se comporta de modo anómalo, buscando el beneficio propio y degradando la prestación y calidad del servicio proporcionado por la red. En términos generales el ataque puede comprender el fallo o toma de control de varios nodos (Lamport et al., 2019; Arroyo Guardeño et al., 2019).

Agujero negro: el atacante elimina o descarta paquetes de control de datos seleccionados (o todos) que pasan a través de él, con lo que se pierde parte (o toda) la información.

Inundación: el atacante intenta inundar el enrutamiento que se está utilizando mediante el envío de una gran cantidad de paquetes utilizando una ruta alternativa. Con ello, la ruta legítima decaerá en favor de la empleada por el atacante.

Agujero de gusano: este ataque se produce cuando dos nodos maliciosos anuncian tener un trayecto muy corto entre ellos. El túnel entre ambos nodos es considerado por la red como una buena ruta de datos y es la que algunos de los nodos legítimos pueden usar para comunicarse.

Agujero de gusano de red de superposición bizantina: este ataque es una variante del ataque anterior y se da cuando el ataque de agujero de gusano se extiende a muchos nodos sensores. En tal caso, el ataque proporciona una falsa ilusión a los nodos honestos de que están rodeados de nodos legítimos.

Ataque sybil: es un ataque de suplantación en el que un nodo malicioso se disfraza como un conjunto de nodos reclamando identidades falsas o generando nuevas identidades. Es especialmente dañino en aplicaciones como los sistemas de votación, la evaluación de la reputación y el enrutamiento geográfico, dado que, en tales casos, los nodos se suelen implementar en un entorno no estructurado y distribuido.

Ataque de sumidero: en este ataque, el adversario se hace pasar por un nodo sumidero y atrae todo el tráfico hacia un nodo o un conjunto de nodos bajo su control. Es similar a un ataque de agujero negro en el que el atacante toma el control de algunos nodos comprometidos y anuncia una ruta de enrutamiento falsa, de modo que atrae hacia sus nodos todo el tráfico.

Ataque a la disponibilidad

Denegación de servicio (DoS) y denegación de servicio distribuida (DDoS) son dos tipos de ataques ya mencionados. En este caso, además, se da la circunstancia de que los nodos tienen una capacidad de cómputo limitada, por lo que el éxito se puede conseguir con mayor facilidad.

Inundación de Hello: en este ataque se trata de encontrar vecinos en una red mediante el envío de paquetes Hello. Recibir este paquete indica que un nodo está dentro del rango de comunicación, por lo que un adversario podría enviar este tipo de paquete con la potencia suficiente como para convencer a los nodos del sensor de que está cerca de la comunicación y puede ser un vecino potencial.

Interferencia (jamming): este ataque es uno de los más dañinos en redes inalámbricas. El atacante interrumpe una banda del espectro con un potente transmisor y evita que cualquier miembro de la red en el área afectada transmita o reciba cualquier paquete.

Colisión: cuando se produce una colisión entre nodos, los nodos involucrados deben retransmitir los paquetes afectados por la

colisión, lo que puede llevar a múltiples retransmisiones si las colisiones producidas por el atacante son muchas. De hecho, la energía gastada por el atacante es mucho menor que la gastada por los nodos del sensor, que pueden agotar las baterías y, por tanto, los recursos.

Compromiso del nodo: es también uno de los ataques más comunes y perjudiciales en estas redes. Consiste en capturar los nodos y tratar de obtener de él datos útiles o hasta reprogramarlos para operar a favor del atacante.

Buenas prácticas

El decálogo de recomendaciones de seguridad en la IoT propuesto por el CCN (CC-IoT, 2017) sugiere tener en cuenta los siguientes consejos:

Evitar el uso de dispositivos IoT cuando que no sean estrictamente necesarios.

No se deben utilizar, en la medida de lo posible, dispositivos IoT que transmitan información a servidores externos[37].

Cambiar las contraseñas que vienen por defecto en los dispositivos IoT por otras realmente robustas.

Actualizar los dispositivos con las últimas versiones disponibles de software y firmware[38].

Desactivar las conectividades remotas de los dispositivos cuando no se vayan a utilizar.

Mantener abiertos solo los puertos de comunicación que sean realmente necesarios.

En el caso de que los dispositivos IoT no permitan una

configuración de su seguridad, solo se debe operar con ellos en una red de área local y tras un enrutador correctamente configurado que sí provea seguridad.

Asegurar la autenticidad, confidencialidad e integridad en todas las comunicaciones locales en la medida de lo posible, especialmente si se realizan por enlaces radio (wifi, bluetooth, etc.). Se conocen ataques a televisiones inteligentes Samsung por una autenticación débil derivada de una validación incorrecta del certificado[39].

Comprobar periódicamente la configuración de seguridad de todos los elementos de la arquitectura IoT y de sus dispositivos de comunicación con el exterior.

Comprobar la visibilidad de los dispositivos propios en buscadores de dispositivos IoT como puede ser Shodan[40].

Infraestructuras críticas

Nuestra sociedad ha crecido tanto en sus aspectos tecnológicos que hoy en día resulta difícil renunciar a muchos de los beneficios que nos han aportado sus implementaciones, desde los puramente personales hasta los que nos afectan como parte de una sociedad. Así, nuestro estilo de vida se basa en las prestaciones de servicios relacionados con los suministros y las comunicaciones a las que tenemos acceso. Estos servicios esenciales de sectores estratégicos (energía, agua, transporte, financiero, TIC, administración, salud, investigación, alimentación, químico, nuclear y espacio)[41], son prestados por un conjunto de infraestructuras públicas y privadas, que se consideran esenciales o críticas. Esta denominación viene del hecho de que la falta o interrupción de su funcionamiento puede ocasionar graves inconvenientes en el desarrollo diario de las actividades básicas de una sociedad.

Estas infraestructuras constan de instalaciones, redes, equipos y tecnologías de la información y las comunicaciones en las que se apoya el correcto funcionamiento de los servicios esenciales de la sociedad, como la salud, la seguridad y el bienestar social y económico, entre otros (NIST, 2018; Vacca, 2017b: parte XIII, caps. 81-84; CCI, 2013).

Hasta ahora hemos comentado los riesgos y amenazas que se pueden presentar en los diferentes ámbitos tratados. Sin embargo, en el caso de las IC, estos riesgos tienen una mayor repercusión al afectar a una gran cantidad de ciudadanos atentando contra la propia estructura y funcionamiento de la sociedad. En este sentido podríamos decir que son más atractivos para los posibles ciberatacantes, fundamentalmente ciberterroristas y grupos organizados que atacan las IC de un país para colapsarlo. Dada su envergadura y complejidad, ataques a escala nacional de servicios de IC exceden la capacidad de operación de sujetos aislados, aunque sí podrían efectuarse este tipo de ataques en una escala local con un

impacto muy acotado geográficamente.

Por otra parte, determinados ciberataques están bajo el amparo de algunos Estados que pretenden desestabilizar a otros, por lo que ya no se trata de un problema nacional, sino que todos los países son susceptibles de ciberataques masivos, lo que ha obligado a establecer alianzas y a compartir información entre países aliados con el fin de minimizar las repercusiones de estos ciberataques. Este hecho es especialmente relevante en el ámbito europeo. El responsable de esta coordinación nacional e internacional es el CNPIC (véase el apartado "Organizaciones de apoyo a la ciberseguridad").

Los principales riesgos y amenazas contra las IC son las que tienen su origen en actos deliberados, ya sean físicos sobre las propias infraestructuras o bien mediante ciberataques, que son los más probables, debido a la enorme evolución de la tecnología.

Las principales amenazas que comprometen la seguridad nacional son las siguientes:

Conflictos armados: es una de las más importantes amenazas a la seguridad nacional, dado que ya no se trata solo del uso de armas convencionales (terrestres, aéreas, marítimas o espaciales) en zonas de alta inestabilidad o gobiernos débiles, sino que las armas se han extendido al ciberespacio. Estas ciberamenazas no solo pueden proceder de sectores estatales, sino de grupos de atacantes muy bien organizados y con abundantes recursos que pueden llevar a cabo actos de sabotaje, desestabilización, desinformación, presiones económicas, etc.

Terrorismo: esta amenaza, cada vez mayor, sobre todo el de procedencia yihadista por su elevado radicalismo, es una de las mayores preocupaciones contra la seguridad de las IC, dada la creciente preparación y especialización de sus cibercomandos en el campo del ciberterrorismo. Cada vez es más sencillo acceder a tecnología que, mal empleada, les permite un mayor adiestramiento, propaganda y les suministra fondos con los que llevar a cabo sus atentados. Por ello, los Estados cada día comparten mayor cantidad de información sobre ciberterrorismo para paliar

esta amenaza.

Crimen organizado: al igual que el terrorismo, esta amenaza es internacional y trata de debilitar a los Estados mediante delitos relacionados con la trata de seres humanos, blanqueo de capitales, tráfico de drogas, etc. En los últimos tiempos los diferentes servicios de información han detectado conexiones entre el crimen organizado y terroristas, lo que agrava aún más esta amenaza.

Proliferación de armas de destrucción masiva: estas armas químicas, nucleares, radiológicas y biológicas suponen una gran amenaza a la seguridad de los Estados. Al hecho de las enormes repercusiones que tendría un conflicto de este tipo entre países, se une la amenaza de que esta proliferación pueda incrementarse con el acceso a tales armas por parte de ciberterroristas.

Espionaje: también en esta amenaza la tecnología ha supuesto una sofisticación en los métodos de espionaje. De hecho, el ciberespacio es hoy uno de los lugares donde mayor proliferación de espionaje se detecta. El ciberespionaje ya no es cosa solo de Estados sino de grupos organizados que venden sus capacidades para acceder a información confidencial y datos sensibles. Los objetivos de este espionaje no son ya solo los Estados sino las empresas. Debe tenerse en cuenta que acceder al conocimiento tecnológico del tejido empresarial de un país permite a la competencia obtener ventajas de todo tipo.

Capítulo 3

Ámbitos de uso

En el capítulo anterior hemos visto los diferentes ámbitos de la ciberseguridad, poniendo de manifiesto que muchos de los ataques contra los diferentes sistemas no distinguen entre el tipo de usuario y se centran, sobre todo, en las posibles vulnerabilidades de los sistemas conectados a Internet, de modo que puedan dirigir contra ellos sus ataques.

En este capítulo se abordarán los principales ámbitos de uso de la ciberseguridad, esto es, los principales aspectos relacionados con la gestión personal, empresarial y de seguridad nacional (gubernamental) de la información. Cada uno de estos ámbitos de aplicación es susceptible de ser atacado por diferentes tipologías de ciberdelincuentes, según su procedencia y los beneficios que se busquen. Los ataques podrán ser más o menos efectivos, según el uso negligente o eficiente de las tecnologías empleadas o de las posibles vulnerabilidades de estas últimas[42].

Tabla 4

Tipos de atacantes, tipo de acción y víctimas, 2018.

Víctima atacada	Gobierno y AAPP	Infraestructuras críticas	Empresas	Ciudadanos
Estados y grupos patrocinados por Estados	Espionaje Sabotaje Interrupción de servicios Manipulación de información Manipulación de sistemas	Espionaje Sabotaje Interrupción de servicios Manipulación de información Manipulación de sistemas	Espionaje	Espionaje
Acciones híbridas	Espionaje			
Delincuentes	Interrupción de servicios Manipulación de información Robo de información	Interrupción de servicios Manipulación de información Robo de información	Robo de información	Manipulación de sistemas
Terroristas	Sabotaje	Sabotaje Interrupción de servicios Manipulación de sistemas Robo de información		

Piratas políticos
Manipulación
Cibervándalos
Robo de información
Personal interno (contratistas)
Interrupción de servicios

La mayor parte de los informes de ciberseguridad señalan un incremento en el número de agentes de las amenazas, esto es, de entidades que explotan una vulnerabilidad, ya sean humanas o no. Las razones que se apuntan son varias: accesibilidad y compartición de nuevas herramientas de ataque, dificultad para probar la autoría del ataque y colaboración entre grupos de atacantes.

Por otra parte, en el informe sobre el panorama de amenazas de 2018, ENISA presenta información sobre las amenazas más significativas, según el tipo de actor y el vector de ataque usado (ENISA, 2019). En este informe destaca en primera posición el malware, seguido por los ataques basados en webs fraudulentas, ataques a aplicaciones web, phishing, el nuevo ataque denominado vishing[43], denegación de servicio, spam, botnets, violaciones de las políticas de acceso a datos, personal interno (insiders) y manipulación física/daño/robo/pérdida.

En esta lucha contra las amenazas de la ciberseguridad, es importante destacar la existencia de estructuras básicas de gestión, nacionales e internacionales, de estas ciberamenazas. De hecho, de acuerdo con la Directiva 2016/1148 NIS del Parlamento Europeo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, existe una red de equipos de respuesta a incidentes de seguridad informática (CSIRT, computer security incident response team) con el objetivo de combatir de modo coordinado las ciberamenazas[44].

Para terminar esta introducción, es preciso destacar que las amenazas y los ataques buscan su mayor rendimiento, por lo que en general no distinguen si sus posibles víctimas pertenecen a un ámbito u otro. No obstante, con el fin de que el seguimiento de este libro resulte más sencillo al lector, nos hemos tomado la libertad de incluir las amenazas y los ataques en los tres diferentes ámbitos considerados, según la popularidad de tales amenazas y sus ataques asociados. Si bien el enfoque que hemos dado al ámbito de la gestión personal de la información va más dirigido a la protección de los datos de los individuos y su privacidad que en las otras dos secciones.

Gestión personal de la información

Para tener una idea del uso de Internet en el mundo, basta considerar que, en el primer cuatrimestre de 2020 se estimó que la población mundial era de casi de 7.797 millones de habitantes, mientras que el número de usuarios con acceso a Internet en todo el mundo, en la misma fecha, era de algo más de 4.648 millones de personas. Esto es, según estas cifras, el 59,6% de la población mundial utiliza Internet. No obstante, la distribución por regiones es muy diferente, como muestra la tabla 5 (IWS, 2020). Así, el 50,9% de los usuarios mundiales conectados procede de Asia, lo que supone el 55,1% de su población; mientras que el 7,5% de los internautas son estadounidenses, representando el 94,6% de su población. En el caso de Europa, el 87,2% de los europeos son usuarios de Internet, siendo el total de europeos el 10,7% de la población mundial.

Tabla 5

Distribución de población mundial y usuarios con acceso a Internet, por regiones, mayo de 2020.

Región	Población estimada (2020)	Porcentaje (%) de población mundial	Usuarios de Internet (2020)	Porcentaje (%) de usuarios de Internet	Tasa de penetración (%)
África	1.340.598.447	17,1	2.366.213.308	50,9	11,3
Asia	4.294.516.659	55,1	2.366.213.308	50,9	55,1
Europa	834.995.197	10,7	727.848.547	87,2	15,7
Latinoamérica y Caribe	658.345.826	8,5	453.702.292	68,9	10,0
Medio Este	260.991.690	3,3	183.212.099	70,2	3,9
América del Norte	368.869.644	4,7	348.908.868	94,6	7,5
Oceanía y Australia	42.680.380	0,5	28.917.600	67,7	0,6
Total mundial	7.796.949.700	100	4.648.228.067	59,6	100

Las anteriores cifras muestran cómo se distribuyen los internautas en el mundo y el gran potencial y posibles beneficios que puede suponer conseguir que un pequeño porcentaje de los usuarios que acceden a Internet sean víctimas de un ciberataque.

Ello nos da una idea del enorme interés que puede suponer que los usuarios sean vulnerables a diferentes ataques, máxime cuando los atacantes son conscientes de la poca o nula protección en seguridad que la mayor parte de los usuarios instala en sus ordenadores.

Por otra parte, el World Economic Forum (WEF), en su informe sobre riesgos globales (WEF, 2019) señala que uno de los riesgos más importantes en la economía mundial es el de los ciberataques. De hecho, en este informe, el fraude y robo masivo de datos aparece en cuarto lugar, mientras que los ciberataques son el quinto riesgo a nivel mundial.

Así pues, la seguridad, que afecta a toda nuestra sociedad, debe comenzar por establecer unos mínimos umbrales que protejan los datos y equipos de los usuarios. La gestión personal de la seguridad hace referencia a los métodos, aplicaciones y servicios que como usuarios tenemos a nuestra disposición con el fin de proteger nuestros datos y nuestra privacidad.

Amenazas

A lo largo de esta sección mostraremos las diferentes amenazas que nos pueden afectar como usuarios y las diferentes formas que tenemos de combatirlas y paliar sus efectos:

Robo de datos personales y ataques a la privacidad: los informes y análisis de los últimos años señalan una tendencia en el incremento de los ataques contra los datos personales. Los atacantes ya no son solo piratas o ciberdelincuentes, ahora también se han unido a este

ataque determinados Estados. El principal objetivo de estos ataques son los fraudes (robos con tarjetas o accesos a bancos), el robo de identidades para llevar a cabo suplantaciones con los que ejecutar otros ataques, etc. Es más, en muchos casos no es necesario violentar los sistemas de protección de los datos para hacer un uso ilegítimo de los mismos. Existen múltiples ejemplos en los que los proveedores de servicio emplean los datos de sus clientes sin contar con su consentimiento. El caso de Cambridge Analytica representa un suceso paradigmático de abuso en el acceso y explotación de datos personales de usuarios[45]. Cambridge Analytica recopiló más de 50 millones de datos de usuarios de Facebook, haciendo posible conocer sus actividades en las redes sociales y luego utilizar tal información para enviar masivamente anuncios políticos durante las elecciones presidenciales de 2016 en Estados Unidos.

Desinformación e información imprecisa o de mala calidad: el uso de noticias falsas (fake news) y su distribución a través de redes sociales y mensajería instantánea pretende influir en las opiniones y el comportamiento de los ciudadanos. De hecho, el uso de técnicas de análisis de big data aplicadas a la información recopilada de redes como Facebook, Twitter, LinkedIn, Instagram, etc., permite desplegar sofisticados ataques (CCN-CERT, 2019a). En este sentido, debe hacerse notar que existen diferencias en cuanto a la manipulación de la información según su intención. Así, en inglés se distingue entre disinformation, misinformation y malinformation (Wardle, 2019). En la conclusión detallaremos las características de estos tipos de “virus informacional” y el ciberriesgo asociado.

Elementos facilitadores: elementos que, sin ser herramientas propias de ataques, en momentos determinados incrementan la accesibilidad o la efectividad de ataques posteriores. Tal es el caso, por ejemplo, de las botnets que se alquilan para determinados ataques, los piratas que intercambian información para facilitar nuevos ataques (datos personales, datos bancarios o tarjetas de crédito), los dispositivos conectados a la IoT que facilitan los ataques por DDoS, etc.

Minería maliciosa de criptomonedas (cryptojacking/cryptomining): esta amenaza ha surgido en los últimos años con motivo del auge de las criptomonedas como bitcoin (Arroyo Guardeño et al., 2019).

Utiliza los recursos computacionales de un dispositivo para minar, esto es, generar criptomonedas, de forma que tiene un objetivo económico. Es un ataque que pasa desapercibido a menos que el usuario repare en la ralentización de su sistema provocado por el minado. Además de un antivirus, existen extensiones de los navegadores web que avisan si un sitio web lo realiza (por ejemplo, en Firefox tenemos NoCoin y NotMINING.org).

Tiempo de reacción: en general, se ha detectado que cuando un ciberataque contra un sistema tiene éxito, la repercusión del mismo es inmediata. Por el contrario, desde que se ha detectado un ataque en un sistema hasta que se detiene y, sobre todo, hasta que ser reparan los daños sufridos pueden pasar días o hasta meses.

Herramientas[46]

De las muchas categorías que pueden considerarse dentro de las tecnologías para la mejora de la privacidad o PET (privacy enhancing technologies), consideramos las cuatro que son más populares:

Mensajería segura (secure messaging): las aplicaciones de mensajería segura tratan de proporcionar una transmisión segura de mensajes instantáneos, es decir, mensajes transmitidos en tiempo real a través de Internet, entre dos o más partes[47]. En general, están diseñadas para mejorar la privacidad de las comunicaciones de manera que ningún tercero no autorizado pueda acceder al contenido de las comunicaciones (texto, voz, imagen, vídeo, etc.). Con el fin de proteger las comunicaciones del usuario, las aplicaciones de mensajería segura utilizan protocolos y algoritmos criptográficos para el cifrado de extremo a extremo (E2E o end to end)[48]. Este tipo de cifrado E2E, como el protocolo Double Rachet[49], garantiza que solo los usuarios que se comunican tienen acceso al contenido de la comunicación. Además, el cifrado entre cliente y servidor asegura el transporte de datos entre el dispositivo

de los usuarios y cualquier servidor del proveedor de los servicios de mensajería. Otra característica de estas herramientas es el almacenamiento cifrado de los datos. Existe una extensa variedad de aplicaciones de mensajería segura disponibles para diferentes sistemas operativos y plataformas, especialmente en el sector de los smartphones: WhatsApp, Telegram, Signal, Riot.im, Wire, Chatsecure, Threema y Wickr (en el apartado "Requisitos específicos" del capítulo 4 se analizarán los pros y contras de estas soluciones, en términos de centralización, disponibilidad del código fuente, etc.)

Redes privadas virtuales (VPN, virtual private networks): se trata de una tecnología de red que crea una conexión cifrada a través de una red pública (por ejemplo, Internet) o una red privada de un proveedor de servicios. Las VPN son ampliamente utilizadas por empresas y organizaciones para que usuarios remotos (por ejemplo, empleados) se conecten a su red privada. Se trata de establecer un túnel cifrado que permita al usuario dirigir el tráfico de su comunicación hacia el proveedor de servicios antes de conectarse a Internet. Al establecer este túnel, la VPN puede ocultar la dirección IP del usuario, de modo que quienes están fuera del túnel solo pueden ver la dirección IP del proveedor de servicios VPN. Con ello se consigue que la actividad en la red del usuario (sitios web visitados, correos recibidos, etc.) esté protegida. No obstante, debe quedar claro que el proveedor de la VPN podría identificar tanto al usuario como a su actividad en línea, por lo que la confianza en el proveedor de la VPN debe ser total. Hay una gran cantidad de servicios ofrecidos por muchos proveedores de VPN con el fin de satisfacer las diferentes necesidades de los usuarios[50].

Redes para el anonimato (anonymizing networks): estas redes permiten anonimizar el tráfico de las comunicaciones de Internet (no la identidad de quien interviene ni el contenido) de manera que sea difícil vincular las partes que intervienen en una comunicación, como, por ejemplo, un usuario con la página web que está visitando. Las redes que ofrecen esta funcionalidad se basan, en general, en una red superpuestamente distribuida y en el llamado enrutamiento de cebolla (onion routing). La red de este tipo más conocida es, sin duda, TOR (The Onion Router), que envía el tráfico de la comunicación a través de varios nodos diferentes (al menos

tres) seleccionados al azar, cifrando los paquetes de comunicación en cada nodo. De este modo, cada nodo sabe de dónde viene el paquete y a qué nodo va, pero ignora la ruta completa. Así, la identidad del usuario original queda oculta para cualquiera que observe la comunicación. Otras redes conocidas son JAP (Java Anon Proxy o JonDonym) e I2P (Invisible Internet Project). Algunas aplicaciones móviles que permiten el uso de estas redes de anonimato, basadas en TOR, son Orbot, Orfox, Fire.onion y Orxy. Además de la protección del anonimato, estas redes pueden proporcionar el cifrado de la comunicación a través de la red (caso de TOR), lo que no significa cifrar la comunicación E2E, es decir, entre el dispositivo del usuario y el destino final.

Herramientas antiseguimiento (anti-tracking tools): casi todos hemos notado que, poco después de haber consultado una web para buscar un hotel, un vuelo, un curso, etc., cuando visitamos otra web para algo tan distinto como leer las noticias, por ejemplo, vemos que dicha página nos ofrece publicidad sobre eso que habíamos consultado poco tiempo antes. Esto se debe a que hemos sido víctimas de un seguimiento. Este seguimiento en línea de un individuo es una técnica que permite recopilar información cuando dicho usuario navega en Internet. La información recopilada puede detectar los intereses de un usuario cuando visita determinadas páginas web o determinados factores de su vida privada, como su ubicación, intereses personales, relaciones sociales, datos confidenciales sobre su salud, creencias políticas o preferencias sexuales. Este seguimiento se lleva a cabo mediante rastreadores que emplean desde cookies hasta la captura de la huella digital del dispositivo donde se usa, las redes wifi o los dispositivos bluetooth a los que se conecta. Las herramientas antiseguimiento están diseñadas para bloquear los intentos de estos rastreadores y suelen ser extensiones o complementos de los navegadores que, generalmente, bloquean elementos como scripts, ventanas emergentes, cookies, botones sociales, anuncios, etc.

Algunos ejemplos de complementos de navegadores para ordenadores domésticos son: Ghostery, Disconnect, uBlock origin, Privacy Badger, NoScript, AdBlockPlus, etc. Para los dispositivos móviles existen el modo privado de la navegación de Firefox, Ghostery Privacy Browser, Maxthon Web Browser y Disconnect

Privacy Pro. Por otra parte, debe tenerse en cuenta que algunas de estas herramientas antiseguimiento puede tener repercusiones negativas en la navegación del usuario al bloquear diferentes tipos de sitios o contenidos en los que pudiéramos estar interesados posteriormente.

Gestión empresarial de los datos

La explotación de las vulnerabilidades de las infraestructuras empresariales es uno de los principales objetivos de los atacantes, en especial el sector bancario, por las repercusiones económicas y de lucro que pueden suponer. La herramienta de NetBlocks COST (cost of shutdown tool) estima el impacto económico en cada país que puede suponer la interrupción de Internet, un apagón de datos móviles o una restricción de la aplicación en un determinado lapso[51]. Por ejemplo, este coste durante 24 horas le supondría a España 1.395.909.434 euros. Otro dato interesante es que según estimaciones de McAfee (CCN-CERT, 2019c), el ciberdelito, en la actualidad, puede estar representando un coste mundial cercano a los 600.000 millones de dólares (o el 0,8% del PIB mundial).

Amenazas y vulnerabilidades

Hardware y software de nueva adquisición: las principales razones por las que tanto el hardware como el software pueden considerarse amenazas se debe a una mayor complejidad de las aplicaciones para las que el usuario no está convenientemente formado, a la adquisición de un hardware o software nuevo que aún no ha tenido tiempo de ser analizado o cuyas características se mantienen en secreto por parte de sus creadores (aquí se incluyen los dispositivos móviles), al software que no está completamente actualizado, a la aceptación e integración de elementos de origen externo que no han sido lo suficientemente controlados y a la búsqueda de la eficiencia y velocidad de proceso en detrimento de la seguridad.

La externalización de procesos en la cadena de producción del hardware hace que la matriz de amenazas se incremente. De hecho, el riesgo está asociado no solo al producto final, sino a cada uno de

los actores involucrados en el proceso de fabricación de un producto. En el caso del software sucede algo parecido debido, por ejemplo, a la integración en programas y aplicaciones de las bibliotecas desarrolladas por terceros. Esta integración continua de software debe dar cuenta de la confianza y dependencia depositada en actores externos. Si tal confianza no es evaluada adecuadamente, existe una amenaza que pudiera ser explotada, por ejemplo, a modo de inclusión de alguna suerte de puerta trasera en el sistema o de una falla intencionada que habilitara ulteriores fallos funcionales o vías de ataque por denegación de servicio[52].

A modo ilustrativo, conviene citar las vulnerabilidades, conocidas a comienzos de 2018, como Spectre y Meltdown[53]. Estas vulnerabilidades corresponden a nuevos tipos de ataques contra las modernas arquitecturas de CPU (central processing unit) cuyas áreas protegidas de memoria pueden ser leídas. De hecho, la mayor parte de los fabricantes (Intel, AMD y ARM) se han visto afectados. Las razones hay que buscarlas en que en estas arquitecturas se prima el incremento de su eficiencia y la disminución de costes sin invertir lo suficiente en seguridad. Este tipo de ataques sigue proliferando con nuevas versiones (CacheOut, SGAxe, LVI) y capacidades, por lo que las CPU siguen siendo vulnerables[54]. Ello permite a los atacantes explotar estas vulnerabilidades para filtrar datos confidenciales.

A nivel software, cabe destacar que en 2018 se encontraron vulnerabilidades en las implementaciones de los estándares de cifrado de correo electrónico OpenPGP y S/MIME, que permitían a los atacantes manipular correos electrónicos cifrados, de modo que eran descifrados por el destinatario y a continuación eran reenviados como textos sin cifrar[55].

Dispositivos propios en entornos empresariales: desde hace unos años, los dispositivos BOYD (bring your own device), esto es, dispositivos personales que se utilizan con fines empresariales, se han convertido en algo muy común en muchas empresas. La proliferación de estos dispositivos reduce costes empresariales y parece mejorar la eficiencia y la productividad, dado que el empleado puede contestar correos, trabajar con información de la compañía cuando viaja, está fuera de su oficina o incluso durante su

tiempo libre. Sin embargo, esta tendencia parece que está empezando a disminuir por la falta de seguridad de tales dispositivos y por el hecho de que las empresas se han dado cuenta de que permitir que se acceda a sus redes con dispositivos no corporativos puede suponer un enorme riesgo de seguridad.

DDoS: si bien este tipo de ataque ha decaído en los últimos tiempos, sigue siendo uno de los más importantes, en especial en la industria de los videojuegos. Su principal método de ataque ha sido, tradicionalmente, a través del uso masivo de dispositivos conectados a la IoT, pero también es posible llevarlos a cabo utilizando otros dispositivos, como los móviles, sobre todo si no están protegidos convenientemente. Estos ataques son cada vez más sofisticados y se lanzan desde cualquier parte del mundo, llegando a atacar a muchos objetivos a la vez.

Uno de los ataques de mayor impacto que se ha desarrollado consistió en la generación de tráfico de red de más de 1,35 terabits por segundo contra la plataforma web de proyectos colaborativos GitHub[56].

Dispositivos médicos implantables (IMD, implantable medical device): este tipo de dispositivos sanitarios son dispositivos electrónicos implantados (o semiimplantados) en un cuerpo humano que tienen capacidad para comunicarse, bien vía Internet o mediante telemetría. De este modo es posible que los médicos puedan acceder a los datos del paciente y comunicarse con el sistema implantado (incluso en remoto) con el fin de tratar un problema médico específico o hacer uso de una comunicación inalámbrica para ajustar los parámetros del dispositivo sin tener que realizar una intervención quirúrgica. Los IMD se suelen clasificar en cuatro clases: dispositivos implantados cardiacos y auditivos (marcapasos y desfibriladores, conducción ósea y cocleares), neuroestimuladores (Parkinson, epilepsia), sistemas de administración de fármacos (bombas de insulina o morfina) y biosensores (hemodiálisis, registro de analitos).

Al margen de los muchos beneficios de estos dispositivos, es importante señalar que también pueden suponer diferentes riesgos tanto de seguridad como de privacidad para el paciente. Se ha probado que algunos IMD son vulnerables a ciberataques, ya sea

porque permiten accesos no autorizados a los datos privados del paciente por fallar en los procesos de autenticación o porque los datos están débilmente cifrados (o directamente sin cifrar). También se ha logrado reprogramar de forma remota algunos dispositivos acortando considerablemente su vida de uso por consumo excesivo de la batería o provocando un malfuncionamiento, lo que puede poner en peligro la vida del paciente.

Pago bancario mediante aplicaciones móviles: cada día es más común que los usuarios paguen sus compras cotidianas en lugar de con tarjetas de crédito con las aplicaciones móviles que les bridan sus entidades bancarias. En estos casos, se debe controlar muy de cerca la seguridad ofrecida por tales aplicaciones, dado su potencial peligro contra la economía de los usuarios.

IoT: ya hemos comentado anteriormente que los dispositivos IoT pueden ser una fuente de ataques debido a la poca atención que se ha puesto, en general, en su seguridad, causando daños directos o indirectos al usuario o siendo utilizado como medio para atacar otros objetivos mediante la creación de botnets.

Amenazas persistentes avanzadas: estas amenazas, también llamadas APT (advanced persistent threat), se dirigen contra empresas e instituciones determinadas con el fin de tener acceso a su red, exfiltrando información y propagando el ataque a otros sistemas. El uso del término “persistente” hace referencia a que las APT requieren de una actuación continua a lo largo de extensos periodos de tiempo para poder ser efectivas. El conjunto de procesos informáticos sigilosos y continuos de una APT se suele colocar en sitios web o en los servidores de actualización de los fabricantes de software, para que cuando los usuarios se descarguen actualizaciones o instalen programas, se ejecute el malware.

Sistemas de control industrial: los ICS (industrial control systems) han sido víctimas de ataques, no específicamente dirigidos contra ellos, pero se han visto afectados por sus conexiones a Internet, siendo infectadas sus estaciones de trabajo, especialmente por ransomware (uno de los más conocidos fue el ataque con WannaCry). Las principales vías de entrada fueron los correos con phishing, los soportes extraíbles (pendrives, etc.) y los sistemas de mantenimiento remoto mal configurados.

Agentes de amenazas

Si bien no puede afirmarse de forma categórica que los agentes de las amenazas se dividan por ámbitos, dado que cualquier agente intentará atacar el sistema que le pueda resultar más provechoso, se puede afirmar que unos agentes tienen mayor predilección por la gestión empresarial de los datos que sobre la gestión de la seguridad nacional. Así, si entre los segundos pueden considerarse los ciberterroristas o los hacktivistas[57] (acrónimo de hacker y activismo), entre los primeros destacan los ciberdelincuentes y el personal interno:

Ciberdelincuentes: son los agentes más activos en el ciberespacio. Se estima que, en 2018, más del 80% de la actividad dañina se debió a este grupo, representando estos ataques el 0,85% del PIB de todo el mundo. Su principal forma de actuación es la propagación de código malware usando el correo electrónico. De hecho, más del 60% del tráfico mundial de correo electrónico en 2018 contenía software dañino y constituyó más del 90% de los ciberataques. Otra tendencia ha sido la mejora en los ataques de phishing mediante técnicas de ingeniería social. Finalmente, se ha detectado una innovación en las plataformas conocidas como ciberdelito-como-servicio (CAAS, cybercrime-as-a-service), que además de mejorar los servicios ofertados, tienen una mayor facilidad de uso.

Personal interno: este grupo de agentes está formado por usuarios normales o con privilegios, insiders, que por negligencia o por maldad pueden resultar dañinos a una empresa u organización. Se estima que alrededor del 25% de los incidentes en entornos corporativos se debe a personal interno. De hecho, las empresas están invirtiendo cada vez más en medidas disuasorias con el fin de reducir esta amenaza. El motivo principal en el caso de acciones maliciosas es el lucro personal; mientras que los daños por negligencia, que es la mayor parte del daño, son la divulgación accidental de datos o errores debidos a una mala configuración.

Aspectos de la seguridad nacional

Existen tres conceptos claves cuando se trata el tema de la seguridad nacional y su relación con la ciberseguridad: la guerra cibernética, las operaciones de información y las amenazas híbridas.

La guerra cibernética, guerra digital o ciberguerra (cyberwarfare) es el uso de la tecnología digital por una nación u organismo internacional para atacar otra nación (Andriole, 2020) con el fin de causar daños relacionados con su tecnología, redes digitales de información, etc., mediante el uso de ciberataques (malware, DoS, etc.). Una de las premisas de esta ciberguerra es que ha equiparado el campo de juego en la industria, en el gobierno y en la defensa nacional. De hecho, las preguntas que han dado lugar a esta situación son similares a las siguientes: ¿por qué gastar diez o veinte mil millones de euros en un portaaviones cuando es posible que el enemigo lo desactive digitalmente?, ¿para qué gastar miles de millones en I + D de nuevos productos cuando es posible piratear los planes estratégicos del adversario?, etc.

El amplio desarrollo de este nuevo concepto ha dado lugar a que anualmente se celebren una gran cantidad de congresos y simposios relacionados la cyberwarfare[58].

Las operaciones de información (information operations o info ops) son una categoría de operaciones militares de apoyo directo e indirecto cuyos dos objetivos principales son el de proteger y defender la información y los sistemas de información propios y el de afectar a la información y a los sistemas de información del adversario. En definitiva, se trata de influir, interrumpir, modificar, corromper o usurpar la habilidad del adversario a la hora de tomar o comunicar decisiones de cualquier índole, ya sean humanas o automáticas. Además, como las info ops hacen un uso limitado de la violencia, este tipo de operaciones se usan, principalmente, como elemento disuasorio en conflictos armados[59]. Las actividades que forman parte de las operaciones de información son las siguientes[60]:

Operaciones psicológicas o PSYOPS (psychological operations), que hacen uso de técnicas para influir en el comportamiento del enemigo o aliados.

Operaciones de seguridad u OPSEC (operations security), para determinar las acciones propias que pueden ser observadas por el enemigo y cómo se puede obtener información a partir de ellas, para tratar de evitarlo.

Operaciones sobre redes informáticas o CNO (computer networks operations) por las que se trata de adquirir el control de las redes enemigas o degradarlas, para evitar que este tome decisiones y, a la vez, proteger las propias.

Engaño militar o MILDEC (military deception), para suministrar información o indicadores falsos al enemigo para que pierda su capacidad de ataque.

Finalmente, las amenazas híbridas son uno de los principales desafíos de seguridad a los que en la actualidad se están enfrentando las democracias occidentales. Estas amenazas están enmarcadas en fenómenos específicos “híbridos” como la desinformación, la intromisión extranjera en las elecciones y los ciberataques. Todo ello se ve favorecido por las tecnologías y herramientas que impulsan estas amenazas y que se desarrollan a una gran velocidad (Meesen et al., 2020).

Por una razón u otra, la mayor parte de los gobiernos de las democracias consolidadas sufren ataques desarrollados en otros países, ya sean desplegados por los propios Estados o por grupos subvencionados por tales Estados. Los principales objetivos perseguidos por estos ataques son los de conseguir información política y estratégica, siendo sus medios el espionaje, esto es, robar información con el fin de mejorar su posición estratégica, económica, etc., o el sabotaje, es decir, interrumpir la normal prestación de servicios esenciales y tratar de influir en la opinión pública de los países atacados.

Así pues, en cualquiera de los casos anteriores, la estrategia que siguen los atacantes, ya sea por métodos directos o a través de terceros, consiste en utilizar herramientas propias o desarrolladas por otros, además de emplear métodos sencillos que han demostrado buenos resultados (phishing). También es importante señalar que los atacantes juegan con la posibilidad de que un ataque dirigido contra una víctima tenga efectos colaterales que afecten a otras víctimas, no previstas inicialmente.

Debido a estas ciberamenazas y al crecimiento que se detecta cada año, las democracias han instaurado el concepto de "soberanía digital", que puede definirse como "el impulso de un país para recuperar el control sobre sus propios datos y los de sus ciudadanos" (CCN-CERT, 2019c: 15). Este concepto incluye el hecho de que un Estado, con el fin de defenderse de estos ataques, pueda desarrollar sus propias tecnologías y capacidades ofensivas y defensivas de ciberseguridad.

Stuxnet

Dentro de los ataques a la seguridad nacional, uno de ataques de mayor relevancia mundial fue Stuxnet (Langner, 2013). Se trata de un malware que, en 2010, infectó la central nuclear Natanz, en Irán. El propósito del ataque con Stuxnet era retrasar el programa nuclear iraní.

Parece que hubo dos versiones del malware Stuxnet. La primera era un archivo de configuración para el software de los controladores de las válvulas y los sensores de presión que explotaba algunos fallos de la instalación para poder ejecutar sus acciones. Dado que Stuxnet no tenía ningún método de autopropagación, esta infección debió de llevarse a cabo abriendo manualmente el archivo de configuración (con un pendrive o guardado en uno de los portátiles usados para configurar los sistemas).

Cuando Stuxnet se ponía en marcha, tomaba el control del sistema

reemplazando las funciones del sistema y accediendo a las lecturas de los sensores. Bajo determinadas condiciones, el malware entraba en acción grabando 21 segundos de las lecturas de los sensores y reproduciéndolas en un bucle. De este modo, cuando el sistema de control SCADA[61] (instalado en otro ordenador) pedía las lecturas, se le enviaban las reproducidas de Stuxnet, sin que se apreciara un mal funcionamiento.

Si bien la primera versión de Stuxnet parece desarrollada por expertos en la industria, en la segunda se nota la influencia de expertos en seguridad (Langner, 2013). Una diferencia de la segunda versión con respecto a la anterior es que la nueva podía propagarse de un ordenador a otro, haciendo uso de vulnerabilidades de tipo zero-day, si estos estaban en la misma red privada o infectando dispositivos USB. Además, el malware estaba firmado digitalmente con certificados robados, por lo que al instalarse era considerado como un software legítimo.

Esta segunda versión de Stuxnet atacaba el otro punto débil del diseño de la central nuclear: los rotores. Aproximadamente, una vez al mes, el malware tomaba el control del sistema responsable de controlar la velocidad de los rotores, reduciéndola hasta casi pararlos (120 rpm) y luego elevaba la velocidad a su valor normal. Esta diferencia de velocidades hacía que los rotores pasaran por velocidades críticas que los hacían vibrar al entrar en resonancia, estropeándolos y reduciendo su vida útil.

Al margen de las características anteriormente señaladas, Stuxnet no tenía ningún sistema que permitiera a sus controladores desactivarlo, pero como se transmitía entre redes privadas sin discriminación, es muy probable que la misma forma que parece que se utilizó para inyectarlo en la central nuclear (infectando los ordenadores de los contratistas externos) fue como salió de la misma y se expandió a otros ordenadores, llegando a conocerse más tarde.

Esta falta de control parece indicar que sus creadores estaban, de hecho, experimentando para saber hasta dónde se podía llegar con este tipo de ataque, dado que todo indica que era el primer paso de la ciberguerra. De hecho, la importancia de

Stuxnet se debe a que ha sido considerado como la primer ciberarma puesta en marcha por el gobierno de un país contra otro.

Agentes de amenazas

Por un lado, existe el ciberterrorismo y ciberyihadismo, donde las amenazas procedentes de grupos terroristas o hacktivistas parece que se han mantenido estables a lo largo de 2018 y 2019. Los ciberyihadistas se siguen caracterizando por sus acciones de propaganda digital, reclutamiento y recaudación de fondos. No se ha detectado que hayan realizado ningún ciberataque significativo, salvo el robo de alguna información y ataques a determinadas páginas web desfigurándolas.

Además, están los hacktivistas. Este grupo de piratas también ha mantenido una actividad similar a la de años precedentes. Fundamentalmente en campañas de desfiguración de páginas web y ataques DDoS. Su objetivo es el de hacerse notar en los medios, sin que ello lleve aparejado un lucro económico. La mayor parte de su movilización está relacionada contra decisiones políticas que afectan a asuntos nacionales, internacionales, los derechos de las mujeres y la violencia con armas de fuego.

Finalmente, desde el punto de vista de la ciberseguridad nacional, en España tienen competencias el Centro Nacional de Inteligencia (CNI), el Centro Nacional para la Protección de Infraestructuras y Ciberseguridad (CNPIC) y el Mando Conjunto de Ciberdefensa (MCCD). Cada uno de ellos, tiene sus propias funciones según se establece en la normativa vigente (capítulo 1).

Capítulo 4

Soluciones y buenas prácticas de ciberseguridad

Una vez analizados aspectos como el tipo de amenazas, los dominios y los ámbitos de uso, es el momento de centrarse en las soluciones y las prácticas aconsejables para evitar problemas asociados a la ciberseguridad. Pero antes de comentar dichas soluciones y buenas prácticas, es necesario presentar el concepto de software libre y explicar cómo este tipo de desarrollos contribuye a crear y mantener niveles elevados de seguridad.

¿Software libre o software privativo?

En las últimas décadas se ha popularizado el concepto de software libre, que representa todo software cuyo código fuente está disponible de forma que pueda ser estudiado, modificado, utilizado libremente con cualquier fin y redistribuido con o sin cambios. Su definición está asociada al nacimiento del movimiento de software libre, encabezado por Richard Stallman y la fundación de la Free Software Foundation en 1985.

En comparación, el software privativo es aquel en el que el código fuente no está disponible, impidiendo que los usuarios puedan estudiarlo y modificarlo. Debido a su naturaleza comercial, muchas de las aplicaciones que utilizamos día a día son privativas, desde el sistema operativo a las aplicaciones ofimáticas, pasando por los reproductores de música o navegadores de Internet. Algunas de las ventajas del software libre son las siguientes:

Fácil acceso y bajo coste de adquisición (muchas veces gratuito).

No es necesario adquirir nuevas licencias al poder instalar las aplicaciones en tantos equipos como sea necesario. No obstante, existe software libre cuyas actualizaciones sí requieren la obtención de licencias.

Mayor capacidad y flexibilidad para acceder a programas y adaptarlos.

La disponibilidad del código fuente permite auditarlo y verificarlo, lo que habilita la construcción de un espacio colaborativo para la evaluación de la seguridad y fiabilidad de mayor intensidad que en el caso del software privativo. Como ejemplo, baste considerar el caso de la comunidad de “cazadores de fallos” (bug bounters) en software. En el caso del software privativo, esta comunidad ha de

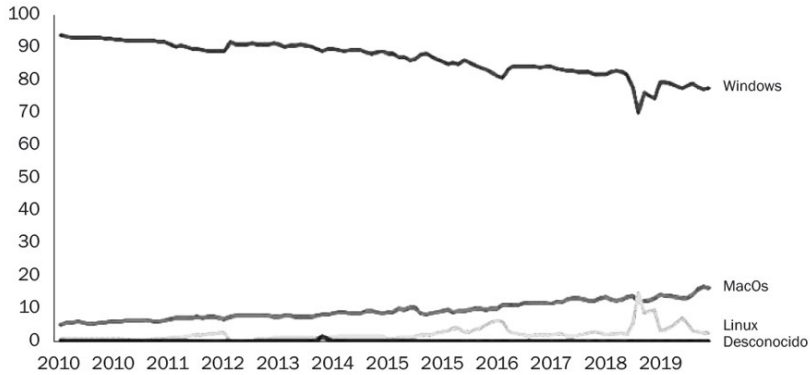
aplicar técnicas complejas de análisis y de ingeniería inversa, mientras que el acceso al código fuente en el caso del software libre simplifica su tarea, aumentando tanto su eficiencia como su eficacia.

El software privativo no es mejor ni peor que el software libre, su calidad depende del esfuerzo empleado en su desarrollo y mantenimiento. Tal y como se puede comprobar en la figura 3, no existe ningún sistema operativo que sea inmune frente al malware o cualquier otra variante de ciberataque.

Lo que sí es cierto es que el hecho de tener acceso al código fuente representa un signo de transparencia y permite identificar posibles vulneraciones de privacidad o factibles brechas de seguridad en el software. Ahora bien, los ciberdelincuentes también tienen acceso inmediato al código fuente en el software libre y, por ello, en ocasiones pueden encontrar fallos de seguridad que pueden aprovechar más fácilmente. Al mismo tiempo, la adopción de enfoques de código abierto abona el principio de transparencia e impide que aparezcan algunos de los efectos colaterales indeseados de las soluciones de seguridad “basadas en la oscuridad”.

Figura 3

Evolución de los ataques a los distintos sistemas operativos de PC.



Fuente: https://www.incibe.es/protege-tu-empresa/blog/los-ordenadores-macos-no-son-invulnerables-sabes-protegerlos

La elección de soluciones de código abierto afecta a todo el ecosistema hardware y software. De hecho, las iniciativas de código abierto también comprenden esfuerzos orientados a promocionar el desarrollo transparente de hardware. Así, se distingue entre productos de software libres y de código abierto (FOSS, free and open source software) y productos de hardware libres y de código abierto (FOSH, free and open source hardware). En el contexto del hardware abierto, cabe destacar el caso de asociaciones como la Open Source Hardware Association (OSHA), empresas como Purism e iniciativas como la European Processor Iniative (EPI). EPI es una propuesta impulsada por la Comisión Europea con el objetivo de promocionar el despliegue de un ecosistema RISC-V, lo que permitiría recuperar la independencia en tecnología de microprocesador que se perdió tras la compra de la europea ARM por parte del grupo japonés Softbank en 2016[62] y su posterior venta en 2020 a Nvidia Corporation[63].

La independencia tecnológica no es una cuestión baladí, con implicaciones no solo a nivel estatal sino también a nivel de usuario, entendiendo a este de forma amplia no solo como consumidor final, sino también como desarrollador de hardware y/o de software.

Herramientas para proteger la privacidad

Actualmente, una de las preocupaciones más importantes es la preservación de la privacidad y de los datos personales mientras se realizan actividades cotidianas como compras electrónicas, operaciones de banca electrónica o envío de mensajes. Esta preocupación ha dado lugar a una creciente aparición de herramientas y aplicaciones que tienen como objetivo ofrecer funcionalidades que ayuden a preservar la privacidad del usuario, como por ejemplo aplicaciones de navegación anónima, protección contra el seguimiento o cifrado de datos.

Sin embargo, en algunos casos, la funcionalidad de estas herramientas puede no ser la esperada, por ejemplo, debido a limitaciones en la operación real de la herramienta o en los mecanismos de mantenimiento. Las aplicaciones de este tipo que fallan en ofrecer lo que prometen pueden constituir un riesgo, ya que la falsa sensación de protección puede provocar la pérdida o compartición de datos personales y afectar negativamente la vida personal y laboral de los usuarios.

Existen multitud de herramientas para mejorar la privacidad de los usuarios, pero no es el objetivo de esta obra recomendar unas u otras, puesto que para dicha tarea ya existen organismos y grupos de trabajo con listados de aplicaciones, como por ejemplo la Electronic Frontier Foundation, EPIC, PRISM break, Me and my shadow o Privacy Tools. En su lugar, pensamos que es más interesante resaltar cuáles son las características que los usuarios deberían valorar más en el momento de tomar la decisión sobre qué aplicaciones de privacidad y seguridad instalar. Existen dos grandes grupos de requisitos: los básicos que comparten todas las herramientas y los específicos que dependen del tipo de aplicación.

Requisitos básicos

Los requisitos básicos a considerar serían: madurez y estabilidad, implementación de políticas de privacidad claras y usabilidad.

Por madurez y estabilidad nos referimos a la forma en que una herramienta responde a los desafíos de seguridad y privacidad tanto existentes como nuevos, así como la manera en que una herramienta evoluciona con el tiempo para abordar las necesidades de seguridad y privacidad de los usuarios.

El tiempo puede ser un elemento útil para determinar la madurez de una aplicación, en el sentido de que las herramientas lanzadas varios años atrás han tenido más posibilidades de probarse y mejorarse. Sin embargo, el tiempo no puede definir por sí solo el nivel de madurez y estabilidad de una aplicación, ya que también es necesario tener en cuenta la forma en que una herramienta responde a los nuevos problemas de seguridad y privacidad o la manera en que la herramienta evoluciona, lo que incluye por ejemplo la frecuencia de sus actualizaciones.

Dos parámetros adicionales a este respecto son el nivel de apoyo que recibe la herramienta por parte de la comunidad de usuarios (lo que en ocasiones se puede medir mediante el número de descargas) y las auditorías y revisiones realizados por organismos, empresas del sector y prensa especializada, así como las acreditaciones, certificaciones y premios asociados a dicho software.

Es muy importante que la política de procesamiento de datos personales de los desarrolladores y distribuidores de las aplicaciones sea clara y transparente. En ese sentido, el usuario debe tener acceso a información que le permita determinar el tipo de datos personales a los que tendrá acceso la herramienta, la frecuencia con que la aplicación accederá a esos datos y el propósito que justifique dicho acceso.

A este respecto, el RGPD hace referencia al almacenamiento, procesamiento, acceso, transferencia y divulgación de los registros de datos de un individuo y afecta a cualquier organización a nivel mundial que procese datos personales de personas de la Unión Europea.

En el caso de que haya tratamiento de datos personales, existe la obligación de que haya concreción, publicidad y transparencia en lo relativo a la política de privacidad. Por otra parte, si los datos del usuario son enviados a un servidor, es imprescindible conocer quién recibirá esos datos, el propósito y contenido de la transferencia de datos y los derechos que tiene el usuario (borrado, rectificación, etc.) sobre los datos una vez han sido transferidos.

Por todo ello, es muy importante que la política de privacidad de los desarrolladores y distribuidores de software esté recogida por escrito de manera completa y pueda ser revisada por cualquier usuario. Igualmente, es fundamental que los usuarios sean informados de cualquier cambio en la política de privacidad durante el tiempo en que usen las aplicaciones.

Es especialmente interesante reseñar el ejemplo que suponen las políticas de uso de cookies. Al navegar por multitud de páginas web, lo primero que ve el usuario es un aviso sobre aceptación de cookies. Estos elementos permiten al dueño del sitio web identificar a los usuarios de manera que la información que se les muestre pueda ser personalizada (contenidos de interés, etc.). Sin embargo, en muchas ocasiones la aceptación de las cookies conlleva la compartición de información del usuario con muchas otras empresas y anunciantes, por lo que es fundamental que dicha aceptación sea el resultado de un proceso informativo pleno y que la no aceptación no suponga una pérdida de funcionalidad para el usuario[64].

La usabilidad define la medida en que los usuarios pueden utilizar una herramienta para aprovechar su funcionalidad de manera satisfactoria y eficaz. La usabilidad suele interpretarse de modo subjetivo como una percepción del usuario final que es difícil de modelar y de integrar en el proceso de diseño, implementación y validación de soluciones de protección y de seguridad en sistemas de información y comunicación. No obstante, es posible establecer un conjunto de métricas para homologar la inclusión del factor humano en la generación de cualquier producto o solución de ciberseguridad. Entre ellas destaca la facilidad durante las etapas de instalación, uso y desinstalación de la herramienta, así como la cantidad de información disponible durante esos procesos.

En el caso de la fase de utilización de la herramienta, es importante evaluar su dificultad de uso, es decir, si es una herramienta fácil de usar para el público en general o, por el contrario, está destinada a usuarios con conocimientos avanzados en la materia, y el empleo de una configuración por defecto que proteja la seguridad y privacidad del usuario. Ello implica que no sea necesario modificar la configuración para obtener los niveles máximos para la protección de su confidencialidad y privacidad.

Requisitos específicos

Los requisitos específicos dependen del tipo de herramienta. En este análisis hemos incluido requisitos asociados a aplicaciones de mensajería instantánea, de navegación anónima y de antiseguimiento.

Las aplicaciones de mensajería instantánea son de las más utilizadas en los teléfonos móviles, tanto en entornos privados como laborales. Para poder comparar las distintas opciones existentes, es conveniente analizar las siguientes características: existencia de cifrado de extremo a extremo (de manera que los datos descifrados no puedan ser leídos por el proveedor de la aplicación), configuración por defecto robusta, seguridad de los datos almacenados en local o en los servidores del proveedor (por ejemplo, las copias de seguridad), implantación de mecanismos de autenticación que garanticen que solo los usuarios legítimos puedan acceder a sus cuentas o la posibilidad de realizar comunicaciones anónimas, de forma que nuestro identificador de usuario no esté ligado a nuestra identidad en el mundo real.

En el diseño de los servicios de mensajería instantánea es posible identificar tres tipos de servicios: centralizados, federados y de igual a igual (P2P o peer-to-peer):

Los servicios centralizados son aquellos en los que cada participante

se encuentra en el mismo servidor o en una red de servidores que están controlados por la misma organización. Las aplicaciones de mensajería WhatsApp o Signal utilizan este esquema. Entre sus ventajas está la mayor facilidad de uso por parte del usuario, mientras que entre sus desventajas destaca el hecho de que, al depender de una única organización, la política de privacidad puede ser modificada provocando una potencial pérdida de derechos para el usuario.

Los servicios federados utilizan múltiples servidores independientes que pueden comunicarse entre sí. La federación permite a los administradores del sistema controlar su propio servidor y seguir siendo parte de la red de comunicaciones más grande. Este esquema se utiliza, por ejemplo, en el correo electrónico. Con este sistema, los usuarios tienen la capacidad de elegir el proveedor que se ajuste mejor a sus necesidades (tanto de usabilidad como de privacidad), mientras que entre los aspectos negativos destaca el hecho de que los distintos proveedores deben permitir el servicio con otros proveedores, lo que en ocasiones puede no ocurrir si algún proveedor deniega el servicio a otro por determinados motivos.

Los servicios P2P se conectan directamente entre sí sin necesidad de servidores de terceros. Los clientes (peers) generalmente se conectan entre sí mediante el uso de una red distribuida, como es el caso de Internet, aunque también existen casos de servicios basadas en proximidad, donde se establece una conexión a través de wifi o bluetooth. Aunque desde el punto de vista de la privacidad pueden parecer los más favorables a los usuarios, a veces es necesario utilizar elementos adicionales para evitar la transmisión de datos que pudieran identificar al usuario.

Llegados a este punto es de interés subrayar que algunos servicios, como es el caso de Element (anteriormente Riot), permiten darse de alta y comunicarse sin asociar nuestro número de teléfono al perfil de usuario. Aunque los desarrolladores de Signal han publicado recientemente que no va a ser necesario vincular una cuenta a un número de teléfono móvil, lo cierto es que solo se sustituye el uso del número de teléfono en la fase de recuperación de la cuenta mediante la utilización de un PIN[65].

Dentro de una disciplina de ofuscación de la identidad, tendría sentido optar por el uso de número de teléfonos desechables (burner phones). Sin embargo, en Europa esta posibilidad llegó a su fin tras los atentados del 11-M en Madrid y del 7-J en Londres. En el caso español, la ley que tipifica la vinculación de una tarjeta SIM a una persona física (esto es, a un DNI) es la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones. No obstante, hay países donde aún se pueden comprar tarjetas SIM sin identificación personal alguna, lo que ha generado un mercado negro de tarjetas SIM cuyo usuario no puede ser identificado.

También existen servicios online de números de teléfono temporales para recepción de SMS[66]. Estos servicios se podrían utilizar, por ejemplo, para recibir el mensaje SMS de confirmación en aplicaciones de mensajería y evitar la identificación de nuestro número de teléfono real, siempre que no sean utilizados en una cierta ventana temporal (algo que por otra parte es difícil de que ocurra).

En definitiva, la elección sobre qué aplicación utilizar, es decir, aceptar una u otra de las arquitecturas mencionadas, depende del usuario, puesto que la percepción de ciberriesgo y el balance entre privacidad y usabilidad es completamente personal.

Bajo la categoría de navegación anónima y segura se pueden incluir tanto las aplicaciones para usar o crear una VPN (virtual private network) como las de navegación anónima (Tor o redes de mezcla de tráfico de red, mixing networks), que deben incluir características técnicas como gestión avanzada de direcciones IP (ofuscación, cambio periódico, etc.), protección contra herramientas de análisis de tráfico, posibilidad de cambiar los nodos de red utilizados o la inclusión de un cortafuegos, todo ello con un rendimiento equiparable al de las conexiones realizadas sin estas aplicaciones.

Las herramientas de antiseguimiento tienen como objetivo evitar que los usuarios puedan ser identificados a partir de la navegación que realicen en Internet. Suelen ser plugins disponibles para los principales navegadores de Internet (Chrome, Firefox, Edge, etc.), pero en ocasiones dan lugar a nuevos navegadores, ya sean

versiones más restrictivas de los mismos navegadores mediante pestañas privadas (Firefox y Chrome) o directamente nuevos navegadores derivados de los más populares con una configuración por defecto más restrictiva (Brave o Vivaldi). Otra opción de alto interés es el proyecto Pi-hole, que promete la eliminación de publicidad tanto en navegadores como en aplicaciones mediante un sistema DNS que evita la utilización de servidores de terceros en la navegación.

Para evaluar estas herramientas conviene analizar las listas de elementos que pueden bloquear y la posibilidad de que los usuarios puedan crear sus propias listas. En cuanto a las consecuencias de usar estas herramientas, los usuarios deben disponer de información clara sobre los posibles efectos en la navegación (páginas que no se muestren o que lo hagan incorrectamente) y sobre la posible pérdida de rendimiento al emplearlas.

Protección de credenciales

De las diferentes técnicas de autenticación (capítulo 1), en la mayor parte de los servicios web se opta por el uso de autenticación basada en algo que conoce el usuario, en concreto una contraseña. Las contraseñas son secuencias de caracteres que dan acceso a los servicios o protegen el contenido de los ficheros almacenados en los ordenadores. Debido a su naturaleza, la pérdida o filtración de contraseñas puede comprometer nuestra privacidad, dando la opción a un usuario ilegítimo de publicar contenido en nuestro nombre en redes sociales, leer y contestar a correos electrónicos haciéndose pasar por nosotros, acceder a nuestras cuentas bancarias de forma online, etc.

Para evitar riesgos derivados de una mala gestión de las contraseñas, es importante seguir estas recomendaciones:

No compartir nunca las contraseñas con otras personas, ya que entonces dejan de ser secretas y no debemos dejar nuestra privacidad en manos de otros, por cercanos que sean.

Asegurar su fortaleza, usando combinaciones de por lo menos ocho caracteres que mezclen números, letras y símbolos. Con el objetivo de alargar la longitud de las contraseñas es posible utilizar reglas mnemotécnicas (primera letra del título de varios libros o películas, etc.) y es importante evitar contraseñas típicas (123456, nombre de la pareja, fecha de nacimiento, etc.).

No utilizar la misma contraseña en diferentes servicios, puesto que en caso de que un atacante obtenga una lista de las contraseñas de un servicio, automáticamente podría utilizar esa contraseña en otro de los servicios que utilicemos.

Como parte del proceso de registro en muchos servicios de Internet,

además de nuestro identificador, datos personales y contraseña, se solicita una pregunta de seguridad con su respuesta. Esta pregunta de seguridad se utiliza cuando olvidamos nuestra contraseña y queremos recuperarla o cambiarla. Por ello, es recomendable registrar respuestas para las preguntas de seguridad que sean tan complejas como las propias contraseñas. De nada sirve emplear una contraseña muy segura en nuestro correo electrónico si la pregunta de seguridad contiene una respuesta sencilla que el atacante puede adivinar.

Utilizar un gestor de contraseñas, ya sea de software libre o privativo[67]. En estas aplicaciones solo necesitaremos recordar una contraseña robusta, que da entrada a la aplicación. El resto de contraseñas se almacenan cifradas y solo se pueden recuperar a partir de la contraseña inicial. Ello permite definir contraseñas largas y seguras para nuestros servicios al no ser necesario recordar cada una de ellas. Existen gestores de contraseñas locales que solo sirven para el dispositivo donde están instalados y otros online que permiten la sincronización de contraseñas entre varios dispositivos, aunque esta funcionalidad suele ser de pago para las aplicaciones que cuentan con ella.

Implementar un ciclo de vida de contraseñas robusto, cambiando las contraseñas de forma regular, especialmente aquellas vinculadas a servicios críticos en los que se gestione y haga uso de datos sensibles. En la definición de esta política es de gran ayuda revisar los registros de actividad que muchos servicios online incorporan y que permiten identificar los accesos que se han realizado a nuestra cuenta, aportando información sobre frecuencia y tipo de dispositivo empleado en los sucesivos accesos o intentos de acceso (Google o Facebook, por ejemplo). Es más, muchos de estos servicios nos informan sobre cambios en la modalidad de acceso a nuestra cuenta, así como de intentos fallidos de acceso. Estos avisos han de ser contemplados como indicios de comportamiento anómalo que, según el caso, nos debiera llevar a valorar un cambio de contraseña. Por último, también es una buena praxis comprobar de modo regular si alguna de nuestras cuentas se ha visto comprometida en ataques recientes. En este punto, es de gran ayuda consultar sitios web como Have I Been Pwned?[68].

Al margen de una u otra solución, lo cierto es que los gestores de contraseñas tienen el problema de ser un punto único de fallo (single point of failure), lo que hace recomendable adoptar sistemas de autenticación de múltiples factores siempre que sea posible, además de revisar los mecanismos de notificación sobre incidencias de seguridad de los servicios. Los medios más usuales de incluir un segundo factor de autenticación son:

Código de uso único OTP (one time password) enviado por SMS a un teléfono móvil.

Código OTP mediante un mensaje de voz por teléfono.

Código OTP enviado a la aplicación Google Authenticator.

Vinculación de una llave USB de seguridad compatible con el estándar FIDO (fast identity online), como por ejemplo una Yubikey o una llave Titan de Google.

Copias de seguridad

Las aplicaciones de backup o copia de seguridad garantizan la disponibilidad de la información ante un fallo físico del dispositivo o del sistema que lo controla, la pérdida del propio dispositivo o el robo de información por parte de un ciberatacante.

En particular, las copias de seguridad son un elemento esencial de la protección frente a ataques ransomware, puesto que en caso de disponer de una copia de nuestros datos el atacante pierde el motivo de extorsión y el usuario puede proceder a la sustitución de los datos cifrados por los de la copia de seguridad. Dicha sustitución, evidentemente, debe efectuarse sin estar conectado a Internet, para evitar que la copia de seguridad sea también cifrada por el atacante.

Para que este mecanismo sea eficaz, las copias de seguridad deben realizarse con la suficiente frecuencia, lo que depende del tipo usuario (una pyme no tendrá la misma cantidad de datos generados cada día que un usuario no profesional). Igualmente, dependiendo de las necesidades del usuario y la importancia de la información, es conveniente recurrir a copias tanto locales como en remoto, puesto que los dispositivos físicos locales son más susceptibles a fallos, pérdida o robo que los servicios de backup remoto.

Es interesante mencionar que las copias de seguridad pueden realizarse de manera manual o de forma automática, lo que garantiza que, en caso de darse la situación, los datos perdidos no excedan la cantidad de tiempo fijada en la copia automática.

Por último, las copias pueden ser totales, de forma que cada vez que se realiza el backup se copia toda la información ubicada en el dispositivo de origen, o incremental, de manera que únicamente se copian los ficheros que han sido creados o

modificados desde la última vez que se realizó una copia de seguridad.

Uso de sistemas de detección de malware y actualización de software

En las etapas iniciales de la informática era muy habitual que el sistema operativo no se actualizara hasta la instalación de la siguiente versión de dicho sistema, normalmente una vez transcurridos varios años. La disponibilidad masiva de Internet cambió este modelo, de manera que empezó a ser habitual que los desarrolladores de los sistemas operativos distribuyeran actualizaciones y parches primero de año en año y, posteriormente, de forma mucho más continua.

En la actualidad, la inmensa mayoría de sistemas operativos de ordenadores y teléfonos móviles son capaces de distribuir de forma masiva a sus usuarios actualizaciones de seguridad y de funcionalidades, realizando estas tareas de forma bastante frecuente. Es más, si existe un sistema operativo que no cuenta con un servicio de mantenimiento que asegure actualizaciones de modo regular y efectivo, deberíamos optar por descartar su adopción. Además, no basta con que exista un servicio activo de actualización y de eliminación de bugs y fallos de seguridad, debe tenerse certeza de que dicho servicio está vigente durante un periodo de tiempo suficientemente amplio. Estos dos factores no son condición suficiente para garantizar la robustez de nuestro sistema frente a todo ciberataque, pero al menos permite alcanzar un nivel razonable de protección de nuestros equipos frente a los últimos ataques descubiertos. Hemos de ser conscientes de que en no pocas ocasiones es difícil determinar el tiempo transcurrido entre el descubrimiento de una vulnerabilidad y el conocimiento de ella por parte del equipo de mantenimiento del sistema operativo encargado de generar los parches adecuados.

Lo dicho antes se puede adaptar a las aplicaciones software dedicadas a la seguridad (antivirus, cortafuegos, etc.) y a cualquier otra aplicación, ya que la existencia de una vulnerabilidad en

cualquier elemento software de nuestros equipos es una potencial puerta de entrada para los ciberatacantes. De ahí la extrema importancia de mantener los equipos informáticos constantemente actualizados, especialmente si dichos equipos se conectan de forma habitual a Internet.

Para facilitar la identificación y corrección de vulnerabilidades software, existen mecanismos de intercambio de evidencias digitales en lo relativo a malware y brechas de seguridad[69]. Uno de los más conocidos es el listado de vulnerabilidades y exposiciones comunes (CVE, common vulnerabilities and exposures), establecido en 1998, que asigna identificadores a las vulnerabilidades que se descubren. Estos identificadores son luego utilizados por los distintos proveedores para informar de los problemas de seguridad que han sido resueltos en una determinada versión o parche de seguridad.

Conviene destacar la transición desde la caracterización estática de ataques y vulnerabilidades, como ocurre en el caso de firmas de virus y modelado basado en indicadores de compromiso o IOC (indicator of compromise), hacia la caracterización más genérica y dinámica de tácticas de ataque. Así, es interesante mencionar MITRE ATT&CK (adversarial tactics, techniques, and common knowledge), lanzado en 2013 como una manera de describir y categorizar los comportamientos de adversarios o atacantes basados en observaciones globales. Estas tácticas, técnicas y conocimiento común de adversarios es una lista estructurada de comportamientos conocidos de los atacantes. Puesto que esta lista intenta ser una representación integral de los comportamientos que los atacantes usan cuando ponen en peligro las redes, es útil como base de medidas sobre la eficiencia de mecanismos defensivos y el impacto de tácticas y estrategias ofensivas, además de ayudar a representar y visualizar información de actividad de red y de registros de actividad o logs.

Herramientas para la recolección de evidencias digitales y la auditoría de sistemas

El incremento del número de dispositivos conectados a Internet ha traído aparejado el incremento de incidentes de seguridad informática. En este sentido, el análisis forense digital utiliza diferentes técnicas con el objetivo de reconstruir la secuencia de eventos que tuvieron lugar en uno o en varios equipos informáticos para que un determinado incidente de seguridad tuviera lugar, permitiendo la identificación, preservación, análisis y presentación de datos válidos dentro de un proceso legal.

Por su parte, la auditoría informática es un proceso que consiste en recoger, reunir y evaluar evidencias para determinar si un sistema de información mantiene la integridad y privacidad de los datos y que los procedimientos utilizados para ello cumplen con las leyes y regulaciones establecidas.

Las herramientas para la recolección de evidencias digitales y la auditoría de sistemas son una pieza clave de la ciberseguridad, ya que permiten reconstruir los hechos ocurridos en un determinado incidente de seguridad y, tras su análisis y la consiguiente detección de errores y puntos vulnerables, tomar las medidas adecuadas para que dichos incidentes no vuelvan a ocurrir.

En este contexto, los peritos informáticos son peritos judiciales cuya principal tarea es asesorar al juez en temas relacionados con la informática en cualquier investigación. La función del perito informático consiste, por tanto, en el análisis de elementos informáticos en busca de datos que puedan constituir una prueba o indicio, manteniendo la cadena de custodia de las evidencias informáticas.

Conclusiones

Principales desafíos de la ciberseguridad

A lo largo de la presente obra hemos tratado de identificar los principales elementos que conforman la disciplina de la ciberseguridad, intentando adoptar un enfoque práctico centrado en subrayar problemas que puede encontrar un usuario, pero también incorporando un conjunto básico de recomendaciones para tratar de superar dichos problemas. La dialéctica entre problemas y soluciones y entre seguridad y privacidad es una constante en el diseño, despliegue y mantenimiento de soluciones y sistemas para la protección de la información, que solo tendrá éxito real y efectivo si se tiene en cuenta su principal componente: el factor humano.

Debe existir una cultura y, por tanto, una educación en el uso responsable de Internet y todas las tecnologías que dan sustrato y sentido al ciberespacio. Tal responsabilidad tiene que estar respaldada por marcos jurídicos y normativos que hagan factible la resolución de eventuales contradicciones entre las posibilidades tecnológicas y la protección de derechos de ciudadanos, empresas, instituciones, países y el resto de actores de la nueva realidad ciberfísica. De nuevo, es preciso realizar un esfuerzo de innovación tanto en la esfera legislativa como en el domino jurídico. Si no es así, se corre el riesgo de que los peligros de la tecnología ciber acaben degradando de modo crítico su espacio de posibilidades.

Las especiales circunstancias que han acompañado la revisión y finalización de este libro, de hecho, ponen de relieve la naturaleza de ese nuevo dominio de interacción social, económica y política que es el ciberespacio. La crisis pandémica de la COVID-19 nos ha forzado a mudarnos al ciberespacio para poder dar continuidad a muchas de las actividades de nuestra rutina. Es cierto que ya existía consciencia sobre el impacto de lo ciber en nuestro día a día.

Sin embargo, tras el inicio del estado de alarma del 14 de marzo de 2020, nuestro trabajo, la docencia y, en gran medida, la compra de alimentos y otros productos, todo ello tuvo que realizarse desde nuestras casas haciendo uso de ordenadores, teléfonos y otros dispositivos electrónicos. Esta experiencia nos permite extraer una serie de conclusiones de alta relevancia.

Ciberriesgos y planes de continuidad en la era de la telesociedad

El confinamiento fue uno de los principales elementos de contención de la propagación de la COVID-19 desde el inicio de la crisis en marzo de 2020. Como consecuencia de esta medida, se desplegaron todo un conjunto de soluciones tecnológicas para mantener un mínimo de actividad en lo relativo a la actividad laboral y al sistema educativo en todos sus niveles. El teletrabajo, cuando ha sido viable, y la enseñanza online han cobrado un peso más que significativo en un plan de continuidad de nuestra sociedad en el periodo de crisis pandémica.

El uso de la videoconferencia ha permitido en este periodo la celebración de reuniones de trabajo y la organización de la actividad empresarial con toda una serie de limitaciones. Entre el abanico de soluciones tecnológicas cabe destacar Zoom, Skype, Teams, etc. El uso de estas soluciones nos ha de llevar a valorar los riesgos que entraña usar un producto de un tercero que puede no haber sido debidamente auditado y verificado. Esta tarea es compleja incluso en el contexto del trabajo presencial, todavía más cuando la continuidad del trabajo de oficina requiere el uso de ordenadores y dispositivos sin contar con soporte técnico especializado. En este contexto, las soluciones de urgencia suelen ser la primera opción, lo que abre el camino de riesgos de seguridad como los anteriormente reseñados.

El uso de aplicaciones para videoconferencias permite seguir manteniendo reuniones, incluso aquellas en las que se discuten cuestiones sensibles que han de mantenerse en secreto. El riesgo de espionaje afecta también a las reuniones presenciales, pero requiere la puesta en marcha de procedimientos y técnicas de alto coste y específicos para cada una de las situaciones. En el caso de reuniones a través de

videoconferencia, si existen problemas de seguridad de un software concreto, todas las reuniones celebradas usando este software estarán afectadas por un riesgo de interceptación de la información sensible intercambiada. Esto es, existiría una vulnerabilidad matriz (Schneier, 2019: 87-88), que puede ser explotada de modo generalizado.

El software que se emplea en videoconferencias puede suponer un riesgo, pero hemos de tener en cuenta que solo es una pieza dentro del complejo del teletrabajo. El teletrabajo constituye todo un reto a la hora de diseñar una política de seguridad, y lo es en situaciones de normalidad, pero mucho más en escenarios de crisis similares al deparado por la COVID-19. En este escenario, el teletrabajo se adoptó en la mayor parte de los casos de modo improvisado, sin una política de seguridad previamente definida y debidamente evaluada. Se estima que, desde marzo de 2020, el incremento en las herramientas de teletrabajo ha sido de un 84%. Sin duda, es deseable que todos los teletrabajadores sigan unas buenas prácticas de ciberhigiene, a saber, evitar la instalación de software no autorizado por los responsables de ciberseguridad, no conectarse a redes wifi públicas, no responder correos sospechosos de phishing, etc. Ahora bien, una buena política de seguridad no asume sin más que esas normas de ciberhigiene se van a cumplir, sino que establece mecanismos de control para salvaguardar la seguridad en caso de incumplimiento. Pues bien, en la crisis de la COVID-19 el teletrabajo se desplegó, en muchos casos, sin que los trabajadores tuvieran arraigada esa disciplina de ciberhigiene y sin que su empresa tuviera diseñada una política de seguridad adecuada. Es más, en muchas situaciones los teletrabajadores tuvieron que utilizar ordenadores y dispositivos propios. Dada la situación de confinamiento generalizado y la limitación de recursos tecnológicos en el hogar, es de suponer que en muchos domicilios los ordenadores tuvieran que ser compartidos entre varios miembros de la unidad familiar. Dado que cada uno de ellos tiene, a priori, una cultura de ciberseguridad distinta y usa la tecnología para objetivos diferentes, esta práctica ha de ser considerada como un riesgo de seguridad adicional.

Si nos hacemos eco del anterior diagnóstico, parece necesario desplegar planes de continuidad de negocio que vayan más allá de la consideración de los escenarios habituales de interrupción de la actividad, de modo que integren la amenaza pandémica. Si de modo general la promoción de la ciberresiliencia en dichos planes es muy dependiente de la ciberconcienciación de los trabajadores, en escenarios de teletrabajo generalizado se agudiza dicha dependencia. Por un lado, es preciso formar de modo adecuado a los potenciales teletrabajadores para que cobren conciencia de los riesgos de ciberseguridad asociados a entornos de trabajo fuera del perímetro de seguridad de su empresa. En este sentido, sería de alto interés la planificación de simulacros y ciberejercicios en los que la interacción con los responsables de ciberseguridad permitiera fortalecer rutinas de ciberhigiene, así como pautas para la resolución de problemas de seguridad con el apoyo telemático de los expertos.

Asumiendo el reto de implicar y motivar a los trabajadores a la hora de participar en estos ejercicios, lo cierto es que, si se ejecutan de modo correcto y de forma regular, pueden servir para disminuir el impacto de ciberataques al mejorar competencias tecnológicas, y para la gestión de factores psicológicos (estrés, ansiedad y falta de concentración debido a distracciones en un entorno distinto del laboral) que pueden ser explotados por ciberatacantes en periodos de crisis. Aquí conviene tener presente que la cadena de ataque habitual incluye estrategias de ingeniería social con el objetivo de erosionar la percepción de ciberriesgo de los usuarios, lo que los haría más proclives a bajar la guardia y ser víctimas de phishing y otras herramientas de distracción que los lleve a instalar software sin evaluación de seguridad, acceder a sitios web asociados a campañas de malware y de robo de información, o ser víctimas de ciberacoso. En este sentido, es de alta relevancia la proliferación de ciberataques y cibercrímenes que Europol registró a lo largo de la crisis de la COVID-19 (Europol, 2020)[70]. Se estima que el incremento de ciberataques por phishing, spam y ransomware relacionados con la COVID-19 desde marzo de 2020 ha sido de un 6.000%. Fomentar una cultura de ciberseguridad y de ciberresiliencia

puede y debe contribuir a reducir estas cifras en posibles crisis futuras.

Confianza y fiabilidad tecnológica

Como hemos destacado en la introducción, nuestra sociedad gira en torno a las TIC, de forma que confía en dichas tecnologías para realizar tareas capitales del día a día. Esa confianza está fundamentalmente amparada por la eficacia de las TIC a la hora de realizar tareas rutinarias con bajo coste a nivel personal. Conviene, eso sí, tener presente que una confianza ciega puede entrañar modelos de dependencia que, eventualmente, reducen nuestra capacidad operativa a la hora de reaccionar frente a amenazas que pueden ir desde la falta de disponibilidad del producto tecnológico que usamos habitualmente para realizar una operación, a la incapacidad para detectar a tiempo fallas funcionales y de seguridad de los sistemas TIC que empleamos[71]. En lo concerniente a fallos de los sistemas TIC, nos vamos a fijar en un dispositivo central para el teletrabajo: el router.

Desde el punto de vista doméstico, el router es el elemento al que conectamos nuestros ordenadores y móviles para poder acceder a Internet. Como cualquier otro dispositivo del ecosistema TIC, los routers han sufrido y sufren multitud de ataques como consecuencia de bugs de distinta naturaleza, así como de fallos de seguridad en el diseño de sus políticas de gestión y control de acceso. En abril de 2020 los routers del fabricante LinkSys fueron objeto de un ataque que aprovechó una vulnerabilidad en el control de acceso[72]. Linksys proporciona un servicio, Linksys Smart WiFi, que permite la configuración del router a través de la nube solo creando una cuenta. El acceso a dicha cuenta está protegido mediante el nombre de usuario y su correspondiente contraseña. Tal y como subrayamos en el capítulo 4, en el contexto actual este procedimiento de autenticación no constituye una buena praxis, siendo recomendable usar MFA o al menos 2FA (autenticación con dos factores o two factor authentication). En el caso de Linksys Smart WiFi era viable realizar un ataque por fuerza bruta que permitía obtener la clave de una cuenta y, por tanto, acceder a la misma, pudiendo configurar el

router vinculado a dicha cuenta. En el ataque que estamos describiendo los atacantes cambiaron la configuración del servicio de DNS (el servicio que traduce la dirección URL que escribimos en la barra del navegador en una dirección IP). Mediante un secuestro DNS (DNS hijacking) un atacante modifica este sistema de traducción de forma que la IP devuelta sea la de un servidor bajo su control o la de un recurso propio que contiene malware. En el caso considerado, cuando el usuario intentaba acceder a ciertas direcciones web era redireccionado a IP que estaban bajo el control del atacante, y en su navegador aparecía un mensaje emergente aparentemente de la Organización Mundial de la Salud (OMS). En dicho mensaje se recomendaba al usuario instalar una aplicación con información de interés sobre COVID-19. Pues bien, si el usuario pulsaba el botón de instalación, se instalaba en el ordenador el troyano Oski que roba y exfiltra contraseñas almacenadas en el navegador web, en el registro de Windows e incluso contraseñas de monederos de criptomonedas.

El incidente de seguridad de los routers de LinkSys muestra un caso en el que unas "simples reglas" de ciberhigiene hubieran preservado la seguridad de los usuarios y empresas afectadas: que el proveedor de servicio hubiera implementado un sistema robusto de autenticación o que el usuario tuviera un antivirus actualizado y dudara de promesas que, sospechosamente, de modo oportuno nos ofrecen una ayuda que no estábamos buscando. Ahora bien, no hay nada "simple" en el orbe del ciberespacio, menos aún en la estela de la ciberseguridad. La complejidad asociada a la interacción entre los sistemas de información, los usuarios y los atacantes hace muy difícil establecer modelos precisos de detección y prevención de ciberamenazas. Los algoritmos, modelos y otros procedimientos matemáticos empleados para identificar y autenticar usuarios, diseñar sistemas antivirus y de detección de intrusos, u otros muchos procedimientos para la automatización de tareas en ciberseguridad, tienen limitaciones que han de ser debidamente consideradas.

Estas limitaciones se han puesto de relieve en el capítulo 1 al hablar de la suplantación de identidad, pero existen otros múltiples ejemplos de las limitaciones de salvaguardas y

contramedidas en ciberseguridad. Un caso especialmente significativo es el de los ataques de día cero (zero day), que escapan a la detección mediante el uso de firmas de antivirus, pero también a la identificación dinámica de amenazas basadas en modelos avanzados de comportamiento de malware. A modo de ilustración, consideraremos el ataque efectuado durante la crisis de la COVID-19 contra el servicio VPN de la empresa SangFor[73], que es ampliamente utilizado por diversas agencias gubernamentales de China.

De acuerdo con los expertos de seguridad de Qihoo 360, a lo largo del mes de marzo y principios de abril de 2020 el grupo APT DarkHotel consiguió comprometer la seguridad de al menos 200 servidores VPN. El APT aprovechó una vulnerabilidad no documentada en la actualización de los clientes VPN del servicio de SangFor, instalando una puerta trasera que establecía una conexión con el servidor C&C para descargar código malicioso que, una vez ejecutado, realizaba un fingerprinting del ordenador o dispositivo infectado, es decir, se llevaba a cabo un proceso de recopilación de información para identificar tal dispositivo, e instalaba bibliotecas en el sistema con objeto de alcanzar la persistencia del ataque. Al margen de los detalles, el análisis de esta brecha de seguridad arroja dos cuestiones de especial interés. En primer lugar, los ciberataques y el cibercrimen afectan a toda la gama de actores en el ciberespacio, desde usuarios sin conocimientos avanzados en ciberseguridad a grandes instituciones y estados que cuentan con profesionales con conocimientos muy profundos sobre la ciberseguridad y las últimas tendencias en cibercrimen, ciberterrorismo y ciberguerra. En segundo lugar, Qihoo 360 concluye que la autoría del ataque corresponde a DarkHotel a partir de técnicas de ingeniería inversa y de análisis del código fuente obtenido. Sin embargo, tal y como indica Brian Bartholomew de Kaspersky, Qihoo 360 no aporta evidencias suficientes sobre el origen y la intención del ataque. Según Bartholomew, el análisis de Qihoo 360 adolece de cierto sesgo de autoconfirmación al enlazar el ataque a SangFor con el llevado a cabo por DarkHotel contra la OMS a principios de 2020, en parte por haberse realizado en plena crisis de la COVID-19. En aquel caso, DarkHotel consiguió acceder a documentos editados mediante Microsoft Office explotando una vulnerabilidad de día cero en Internet Explorer, y con el objetivo de

obtener información sobre tests, vacunas y ensayos clínicos sobre la COVID-19. Es difícil colegir si Qihoo 360 establece correctamente la autoría y la intención del ataque a SangFor, pero sí permite cobrar conciencia de uno de los grandes retos actuales en la ciberseguridad: la ciberatribución, elemento clave en las labores de investigación en ciberinteligencia y en la depuración de responsabilidades en ciberdelitos y operaciones de ciberguerra. Aquí conviene tener en cuenta el arsenal de técnicas de evasión de controles de seguridad y de contramedidas, dentro del cual se encuentran las operaciones de falsa bandera. Estas operaciones las ejecutan de forma encubierta gobiernos, empresas y organizaciones, adoptando el comportamiento de otra institución con el objetivo de hacerla responsable del mismo.

La suplantación de perfiles de "comportamiento normal", tácticas de camuflaje u ocultación de actividad por parte de atacantes y, en general, estrategias de evasión de los sistemas o controles de detección representan otro ámbito de necesaria investigación y perfeccionamiento en ciberseguridad. El éxito de muchos de los procedimientos que los ciberatacantes usan para pasar desapercibidos viene deparado en gran medida por la gran capacidad que el ecosistema TIC proporciona para automatizar tareas. La Minería de Datos (MD), el aprendizaje automático (AA) y la inteligencia artificial (IA) son dominios que permiten transformar datos en información, poniendo las bases para la creación de conocimiento. Los diversos actores del ciberespacio conjugan la tripleta MD-AA-IA a lo largo de la cadena de valor del dato, unas veces para garantizar la seguridad y la protección de los diversos activos de sus sistemas y otras para eludir esos mecanismos de seguridad y protección. De hecho, esa dualidad, de nuevo, remite a una tensión entre objetivos, en este caso, en el dominio cruzado de la inteligencia artificial y la ciberseguridad.

La delimitación de ese dominio es otro de los caballos de batalla para los próximos años, siendo especialmente significativos los avances en la denominada clasificación adversaria (Ríos et al., 2019: 101-102). El aprendizaje automático adversario incluye en el proceso de entrenamiento la presencia de atacantes intentado construir mecanismos automáticos de decisión que sean resilientes frente a la modificación adaptativa de datos que persigue forzar la

toma de decisión con alta incertidumbre, abonando el terreno para posibles técnicas de evasión de los controles defensivos en seguridad. Además, este nuevo corpus teórico permitiría construir modelos de riesgos en ciberseguridad con mayor completitud.

Virus informacional: más allá de las fake news

Marzo de 2020 trajo consigo no solo un virus biológico, sino que también deparó un virus informacional. Lo que popularmente se denomina como fake news no es un fenómeno exclusivo de la crisis pandémica de la COVID-19 y, además, comprenden un espectro mucho más amplio (Wardle, 2019). Así, hay que distinguir entre la generación involuntaria (por falta de conocimiento o de prurito profesional) de información imprecisa y falta de rigor (misinformation), de la creación voluntaria de información inválida y fraudulenta que persigue confundir tanto a los consumidores de noticias como a los creadores de opinión pública (disinformation), así como del uso de información genuina pero que empleada en un contexto determinado puede erosionar la reputación de un gobierno, de una institución o de una empresa (malinformation).

La propagación de la COVID-19 ha generado un espacio de búsqueda de certezas por parte del gran público que ha abrazado las buenas noticias que no siempre estaban debidamente evaluadas por la comunidad científica, así como campañas engañosas al servicio de estrategias de ingeniería social y de operaciones de información llevadas a cabo en el contexto de las amenazas híbridas. Las promesas de soluciones milagrosas, los hilos de noticias sobre el origen de la enfermedad y toda una colección de análisis pseudocientíficos que llevaron a la OMS a hablar de la infodemia como un problema si no tan crítico como la propia pandemia (WHO, 2020), al menos suficientemente grave para el control nacional de la enfermedad y la construcción de contextos de colaboración internacional para la superación de la crisis. Es más, algunos actores involucrados en el diseño de la respuesta gubernamental a la pandemia se han visto afectados (al menos en una primera fase) por fenómenos de misinformation al recibir y tratar trabajos en desarrollo como certeza científica, apoyando decisiones políticas en resultados provisionales en

fase de discusión por parte de la comunidad científica.

Al margen de los detalles del método científico y la construcción de evidencia científica, conviene recordar que el éxito de muchos ciberataques reside en la vulnerabilidad del factor humano, que se intensifica en situaciones de ansiedad y de estrés. La intoxicación informativa ocasiona un agravamiento de tal vulnerabilidad, de forma que las noticias fraudulentas se pueden usar en combinación con campañas de spear phishing orientadas al robo de credenciales o a manipular a la ciudadanía de forma que instale malware. Muchos ataques de ransomware han navegado en la cresta de la infodemia COVID-19 y, aunque no es factible establecer una clara relación causal en todos los casos, no se puede obviar el papel que tiene la desinformación y la propagación de noticias no contrastadas y verificadas en la cadena de ataque de grupos APT y otros agentes de la cibergeopolítica. La coordinación de bots y trols[74] es una pieza central en la expansión de las diversas formas y variantes del virus informacional. Las operaciones de información desplegadas mediante estos actores amplifican la polarización política y erosionan la confianza en fuentes autorizadas de información y noticias, esto es, en instituciones sociales y políticas, medios de comunicación e incluso en el colectivo científico y las agrupaciones de profesionales. Esa quiebra de confianza es aprovechada para generar e identificar objetivos vulnerables en el ciberespacio. Por tanto, es aconsejable considerar la confianza como un activo en sí misma y, en consecuencia, hay que establecer salvaguardas y contramedidas para protegerla.

Ese objetivo de generar "vacunas" contra la desinformación y la información imprecisa está detrás de organismos como la Red Internacional de Verificación de Hechos (International Fact-Checking Network, IFCN). Esta red incluye medios de comunicación de múltiples países que están involucrados en la verificación de noticias. Este proceso se realiza de modo semiautomático combinando el conocimiento experto de los periodistas con el uso de herramientas de procesamiento de lenguaje natural y de aprendizaje automático. El desafío aquí remite de nuevo al problema de atribución cibernética y a la posibilidad de utilizar la

tripleta MD-AA-IA para crear campañas de desinformación muy efectivas y creíbles. Esta tarea se complica aún más si se tiene en cuenta la adopción de herramientas para la escritura automática de texto por parte del sector periodístico (por ejemplo, Quill, Heliograph o Polly), lo que dificulta diferenciar texto genuino de texto generado automáticamente por bots.

La capacidad de imitar la actividad humana mediante IA proporciona grandes beneficios en un sinnúmero de sectores productivos e industriales. La incorporación en la IA de la ciberseguridad da lugar también a problemas derivados de esa automatización. Así, por un lado, tenemos industrias como la del videojuego o la del cine que han conseguido sacar un rendimiento sin precedentes a la capacidad de emular actividad humana mediante algoritmos y complejos modelos matemáticos. Por otro lado, tenemos el fenómeno de las deepfakes, esto es, contenido multimedia generado mediante técnicas de aprendizaje profundo (deep learning) y que se utiliza en campañas de desinformación suplantando material genuino relativo a personajes relevantes o generando de modo fraudulento imágenes y vídeos con noticias controvertidas que, en muchas ocasiones, alimentan la polarización política.

Transición desde una inclusión pasiva en el ciberespacio hacia la constitución del cybernetes

Si necesitamos la tecnología en nuestro día a día, pero no somos capaces de sobreponernos a sus disfuncionalidades y uso abusivo, ¿cómo podemos construir un modelo de gobierno adecuado para el ciberespacio? ¿Es posible pensar en la posibilidad de una buena gobernanza de la telesociedad?

Es difícil y quizás no sea posible dar una respuesta al dilema que plantean las anteriores preguntas. En cualquier caso, como profesionales e investigadores de ciberseguridad nos apremia la obligación de tratar de arrojar un mínimo de luz al respecto. Lo haremos echando mano de la etimología del término "ciberespacio", que tiene su raíz en el griego cybernetes.

Nobert Wiener empleó el término griego cybernetes en la definición de la disciplina de la cibernética (Wiener, 1948). Esta disciplina surge de la mano de Wiener con la intención de estudiar el comportamiento de los seres vivos y, tras ello, diseñar modelos matemáticos capaces de imitar tal comportamiento para poder controlarlo. Esa capacidad de emulación es la que refleja el prefijo ciber en todos los casos de aplicación, entre los que se encuentra el del ciberespacio. Si admitimos una metainterpretación de la introducción de este libro, el ciberespacio configuraría una suerte de simulacro que permite configurar y adoptar decisiones que se traducen en acciones sobre el mundo o espacio físico. Aquí hemos de tener bien en cuenta que esa traslación desde el modelo a la acción se sostiene en el armazón de un simulacro, que depende de la capacidad de extraer datos del mundo físico y convertirlos en información para, en último término, ensanchar el corpus de conocimiento.

Como bien reitera Wiener a lo largo de su obra, la valía de ese conocimiento ha de ser ratificada teniendo en cuenta sus

limitaciones en su correspondiente campo de aplicación. El capítulo 1 nos marca los vectores en los que hemos de identificar las limitaciones de todo simulacro de actuación en ciberseguridad. Tras ello, en los capítulos 2 y 3 hemos explicado el campo de ciberseguridad a través de la identificación de los dominios y ámbitos de uso de la cibertecnología. Finalmente, el capítulo 4 nos proporciona una guía mínima de recomendaciones para superar aquellas limitaciones.

En las secciones precedentes de este último capítulo del libro nos hemos hecho eco del suceso que ha marcado la fase final de redacción del texto: la pandemia de la COVID-19. En concreto, hemos remarcado incidentes de seguridad que han surgido a raíz de un aumento de la superficie de ataque fruto de la adopción del teletrabajo, así como del estado de miedo, ansiedad y estrés de la teleciudadanía y de los actores y agentes involucrados en la gestión de la crisis a nivel nacional e internacional. El hecho de que el virus biológico y el virus cibernético hayan progresado casi a la par nos recuerda la existencia de una realidad ciberfísica en la que ciberespacio y espacio físico son vasos comunicantes e interdependientes.

En ese trasvase entre lo biológico y lo cibernético podemos extraer una serie de lecciones adicionales. En primer lugar, la falta de mascarillas y otros recursos básicos para la atención médica en los inicios de la crisis COVID-19 en Europa nos pone en aviso sobre los problemas de la externalización generalizada de la producción. Esto no es exclusivo del sector biosanitario, siendo muy notorio el impacto de la dependencia respecto a terceros países en el sector tecnológico. En el modelo de telesociedad que se adoptó desde marzo de 2020 en Europa, un grueso muy notorio de los recursos que permitieron dar continuidad al trabajo y la enseñanza estuvieron basados en tecnología no europea, lo cual puede suponer un problema en términos de seguridad nacional. En este sentido, además del proyecto EIP que mencionamos en el capítulo 4, es altamente significativa la iniciativa Gaia-X que Francia y Alemania lanzaron en junio de 2020. El hecho de que todavía en nuestros móviles sigamos empleando el GPS en lugar de utilizar el

sistema europeo de geolocalización Galileo, el fracaso del proyecto Quaero como alternativa a Google y otras series de fallidas iniciativas nos indican que la adopción de Gaia-X como cloud por parte de la ciudadanía europea no es solo una cuestión tecnológica.

En efecto, existe la necesidad de generar una cultura de ciberseguridad que impulse una sólida alfabetización digital y que ayude a los usuarios a identificar aquellas tecnologías que pudieran estar erosionando sus derechos. Entre estos derechos es especialmente significativo el de la privacidad. Tal y como hemos recalcado a lo largo del libro, muchos de los ataques que se efectúan dependen de la capacidad de los atacantes para suplantar usuarios o actores legítimos. Esa estrategia de imitación solo es factible si los atacantes pueden acceder a información sobre el comportamiento de los usuarios o actores que pretenden suplantar. Por este motivo es capital que seamos celosos de nuestra privacidad. Si contribuimos a reducir el volumen de datos de los que dispondrían los atacantes y los adversarios en el tablero cibergeopolítico, estos tendrán más dificultades para entrenar sus modelos de IA y construir operaciones de información para desestabilizar el espacio de toma de decisión en nuestra sociedad.

Para concluir, precisamente hay que cobrar debida conciencia de la construcción de esos derechos de la ciberciudadanía, lo que demanda una actualización de los marcos jurídicos y normativos en el nuevo escenario cibernético de configuración y toma de decisión. Si el RGPD supuso un avance significativo a la hora de dotar al ciudadano de recursos para proteger su privacidad, ahora toca emprender toda una empresa de innovación en la regulación de los diversos marcos de automatización y autonomía tecnológica que depara la tecnificación bajo el paraguas de la IA. En definitiva, hace falta un nuevo giro copernicano para situar al ciudadano, al cybernetes, en el centro del ciberespacio.

Bibliografía

Accenture (2019): "Securing the Digital Economy: Reinventing the Internet for Trust", en https://www.accenture.com/_acnmedia/thought-leadership-assets/pdf/accenture-securing-the-digital-economy-reinventing-the-internet-for-trust.pdf

Adler E. y Halliday, J. (2010): "Wikileaks supporters disrupt visa and mastercard sites in 'operation payback'", The Guardian, 9.

Agencia Europea de Seguridad (ENISA) (2019): "Threat Landscape Report 2018. 15 Top Cyber Threats and Trends", enero, en https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Arroyo Guardeño, D.; Díaz Vico, J. y Hernández Encinas, L. (2019): Blockchain, Colección ¿Qué sabemos de?, CSIC-Los Libros de la Catarata, Madrid.

Centro Criptológico Nacional (CCN-CERT) (2014): "Utilización de servicios en la nube", CCN-STIC 823, diciembre, en https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/541-ccn-stic-823-seguridad-en-entornos-cloud.html

— (2017a): "Internet de las Cosas", CCN-CERT BP/05, junio, en https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2261-ccn-cert-bp-05-internet-de-las-cosas-1/file.html

— (2017b): "Principios y recomendaciones básicas en Ciberseguridad", octubre, en https://www.ucm.es/data/cont/media/www/pag-114974/CCN-CERT_BP_01.pdf

— (2018a): "ENS. Seguridad en Bluetooth", CCN-STIC 837, febrero.

— (2018b): "Guía práctica de seguridad en dispositivos

móviles: iPhone (iOS 12.x)", CCN-STIC 455D, octubre, en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3158-ccn-stic-455d-guia-practica-de-seguridad-en-dispostivos-moviles-iphone-ios-12.html

— (2019a): "Desinformación en el ciberespacio", CCN-CERT BP/13, febrero, en https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3552-ccn-cert-bp-13-desinformacion-en-el-ciberespacio-1/file.html

— (2019b): "Guía práctica de seguridad en dispositivos móviles Android 8", CCN-STIC 453F, marzo, en https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/3579-ccn-stic-453f-guia-practica-de-seguridad-en-dispositvos-moviles-android-8.html

— (2019c): "Ciberamenazas y tendencias. Edición 2019", CCN-CERT IA-13/19, mayo, en https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html

Centro de Ciberseguridad Industrial (2013): "La protección de infraestructuras críticas y la ciberseguridad industrial", en https://www.cci-es.org/documents/10694/331476/documento+PIC+y+CI.pdf/6f4f7e57-4719-4d85-ad27-7218 800ca138

Chamareta, C.; Steyer, V. y Mayer, J. C. (2020): "'Hands off my meter!' when municipalities resist smart meters: Linking arguments and degrees of resistance", Energy Policy, 144, 111556.

Creutzburg, R. (2016): "Wikipedia Handbook of Computer Security and Digital Forensics", Part I - Computer Security, en https://www.researchgate.net/publication/296669124_Wikipedia_Handbook_of_Computer_Security_and_Di_Part_I_-_Computer_Security?channel=doi&linkId=56d778c008aee1aa5f75cc13&showFulltext=true

Departamento de Seguridad Nacional (DSN) (2019): "Estrategia Nacional de Ciberseguridad", en https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Edgar, T. W. y Manz, D. O. (eds.) (2017): Research Methods for Cyber Security, 1ª ed., Syngress, Ámsterdam.

Europol (2020): "Staying safe during COVID-19: what you need to know", en https://www.emcdda.europa.eu/drugs-library/staying-safe-during-covid-19-what-you-need-know-europol_en

Ferguson, J. y Redish, A. (2011): "Wireless communication with implanted medical devices using the conductive properties of the body", Expert Review of Medical Devices, 8, 4, pp. 427-433.

Hamed, T.; Dara, R. y Kremer, S. C. (2017): "Intrusion Detection in Contemporary Environments", en J. R. Vacca (ed.), Computer and Information Security Handbook, Morgan Kaufmann, Elsevier, Cambridge, MA.

Hernández Encinas, L. (2016): La criptografía, Colección ¿Qué sabemos de?, CSIC-Los Libros de la Catarata, Madrid.

Hernández Encinas, L.; Martín Muñoz, A.; Gayoso Martínez, V.; Negrillo Espigares, J.; Sánchez García, J. I.; Castelluccia, C. y Bourka, A. (2015): "Online privacy tools for the general public. Towards a methodology for the evaluation of PETs for internet & mobile users", Agencia Europea de Seguridad, ENISA.

— (2016): "PETs controls matrix. A systematic approach for assessing online and mobile privacy tools", Agencia Europea de Seguridad, ENISA.

Herzog, P. (ed.) (2008): "Hacking exposed Linux: Linux security secrets & solutions", 3ª ed., McGraw-Hill, Nueva York.

Hutchins, E. M.; Cloppert, M. J. y Amin, R. M. (2011): "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Lockheed Martin Corporation, Maryland.

Instituto Nacional de Ciberseguridad (INCIBE) (2011): "Riesgos y amenazas en Cloud Computing", marzo, en https://www.incibe.es/extfrontinteco/img/File/intecocert/

EstudiosInformes/
cert_inf_riesgos_y_amenazas_en_cloud_computing.pdf

— (2016): "Decálogo de buenas prácticas en seguridad móvil", en https://www.incibe.es/protege-tu-empresa/blog/decalogo-buenas-practicas-seguridad-movil

International Data Corporation (IDC) (2020): "Smartphone Market Share", julio, en idc.com/promo/smartphone-market-share/os

Internet World Stats (IWS) (2020): "Usage and Population Statistics", mayo, 2020.

Kantar (2020): "Android vs. iOS", julio, Kantar Worldpanel Comtech, en kantarworldpanel.com/global/smartphone-os-market-share/article

Lamport, L.; Shostak, R. y Pease, M. (2019): "The Byzantine generals problem". Concurrency: The Works of Leslie Lamport, 2019, 203-226

Langner, R. (2013): "To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve", noviembre, en https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf

Lee, T. (2013): "The New York times web site was taken down by DNS hijacking. Here's what that means", The Washington Post.

Meessen, R.; Torossian, B. y Bekkers, F. (2020): "A horizon scan of trends and developments in hybrid conflicts set to shape 2020 and beyond", en https://hcss.nl/report/horizon-scan-trends-and-developments-hybrid-conflicts-set-shape-2020-and-beyond.

National Institute of Standards and Technology (NIST) (2011a): "Guidelines on Security and Privacy in Public Cloud Computing", SP800-144, diciembre, en https://www.nist.gov/publications/guidelines-security-and-privacy-public-cloud-

computing

— (2011b): "The NIST definition of cloud computing", SP800-14, septiembre, en https://csrc.nist.gov/publications/detail/sp/800-145/final

— (2018): "Framework for Improving Critical Infrastructure Cybersecurity", abril, en https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

— (2019): "Considerations for Managing Internet of Things (IoT). Cybersecurity and Privacy Risks", NIST.IR.8228, junio, en https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

— (2020): "National Vulnerability Database", 2020.

Panda Security (2020): "Un tercio del total de los virus informáticos existentes se han creado en los primeros diez meses de 2010", en https://www.pandasecurity.com/es/mediacenter/notas-de-prensa/un-tercio-del-total-de-los-virus-informaticos-existentes-se-han-creado-en-los-primeros-diez-meses-de-2010/

Patil, H. K. y Chen, T. M. (2017) "Wireless Sensor Network Security: The Internet of Things", en J. R. Vacca (ed.), Computer and Information Security Handbook, Morgan Kaufmann, Elsevier, Cambridge, MA.

Ríos Insua, D. y Gómez-Ullate Oteiza, D. (2019): Big data, Colección ¿Qué sabemos de?, CSIC-Los Libros de la Catarata, Madrid.

Scambray, J. y McClure, S. (eds.) (2008): Hacking exposed Windows: Windows security secrets & solutions, 3ª ed., McGraw-Hill, Nueva York.

Schneider, B. (2019): We Have Root: Even More Advice from Schneier on Security, John Wiley & Sons, Inc., Indianápolis.

Secretaría de Estado de Seguridad (SES) (2020): "Estudio sobre

la cibercriminalidad en España en 2019", en http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b

Stallings, W. (2017): "Security for the Internet of Things", en J. R. Vacca (ed.), Computer and Information Security Handbook, Morgan Kaufmann, Elsevier, Cambridge, MA.

Unión Internacional de Comunicaciones (UIT) (2018): "Marco de seguridad para la Internet de las cosas basado en el modelo de pasarela", Serie X: Redes de datos, comunicaciones de sistemas abiertos y seguridad, X1361. Aplicaciones y servicios con seguridad (2)-Seguridad en la Internet de las Cosas (IoT), septiembre.

U. S. Food and Drug Administration (FDA) (2020): "Cybersecurity", en https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity

Vacca, J. R. (ed.) (2017a): Cloud Computing Security. Foundations and Challenges, 3ª ed., CRC Press, Taylor & Francis, Florida.

— (ed.) (2017b): Computer and Information Security Handbook, 3ª ed., Morgan Kaufman Publishers, Elsevier, Cambridge, MA.

Wardle, C. (2019): "Information disorder: 'The techniques we saw in 2016 have evolved'", First Draft, en https://firstdraftnews.org/latest/information-disorder-the-techniques-we-saw-in-2016-have-evolved/

Wiener, N. (1948): Cybernetics or Control and Communication in the Animal and the Machine, Hermann & Cie y MIT Press, París y Cambridge, MA.

World Economic Forum (WEF) (2019): "The Global Risks Report 2019", 14ª ed., en https://www.weforum.org/reports/the-global-risks-report-2019

World Health Organization (WHO) (2020): "Novel Coronavirus (2019-nCoV), Situation Report-13", 2 de febrero.

SITIOS WEB DE INTERÉS

Agencia de la Unión Europea para la Ciberseguridad (EINISA): https://www.enisa.europa.eu/

Centro Criptológico Nacional (CCN): https://www.ccn.cni.es/

Centro Nacional de Inteligencia (CNI): https://www.cni.es

Centro Nacional para la Protección de Infraestructuras y Ciberseguridad (CNPIC): http://www.cnpic.es/

Electronic Frontier Foundation: https://www.eff.org

EPIC: https://www.epic.org

Instituto Nacional de Ciberseguridad (INCIBE): https://www.incibe.es/

Mando Conjunto de Ciberdefensa (MCCD): http://www.emad.mde.es/ciberdefensa

Me and my shadow: https://myshadow.org

Observatorio Español de Delitos Informáticos (OEDI): https://oedi.es/

PRISM break: https://prism-break.org

Privacy Tools: https://www.privacytools.io

Notas

1. Más información en https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

2. La RAE ha aceptado el término “jáquer” como equivalente al hacker inglés. De hecho, considera dos acepciones diferentes (una negativa y otra positiva) para esta palabra. La primera es como pirata informático, esto es, “persona que accede ilegalmente a sistemas informáticos ajenos para apropiárselos u obtener información secreta”. La segunda como “persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora”.

3. La exfiltración es un término utilizado en el ambiente militar que hace referencia a la salida de una determinada área o zona, que suele ser territorio enemigo. El término, en oposición a infiltración, ha pasado a significar, en ambientes de seguridad, la pérdida, fuga o violación de datos o información.

4. Son correo basura los mensajes que se reciben sin haber sido solicitados y que suelen proceder de remitentes no conocidos o falsos. En general, hacen publicidad de artículos que no se han solicitado y que al ser enviados de forma masiva perjudican y molestan al receptor. La acción de enviar estos correos basura se denomina spamming, de ahí que estos mensajes también se conozcan como spam.

5. Véase https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-spear-phishing-suplantando-al-servicio-web-11

6. Existen múltiples canales que ponen a disposición de la comunidad diversos exploits: Exploit-DB, https://www.exploit-db.com/

7. Véase Metasploit, https://www.metasploit.com/

8. En desarrollo software, la ofuscación de código consiste en escribir código fuente de forma que no sea fácilmente interpretable. En el contexto de la ciberseguridad, la ofuscación de código dificulta la aplicación de software antivirus y antimalware, ya que impide el reconocimiento directo de patrones de código vinculados con payloads y patrones de código malicioso conocidos.

9. También existen droppers de una única etapa que no ejecutan directamente un payload, sino que incluyen un instalador que se ejecuta tras la instalación del dropper. Ese instalador es el que acaba insertando en el sistema el malware con el payload.

10. Disponible en https://www.electronicid.eu/es/blog/post/aml5-directiva-anti-blanqueo-capitales/es

11. Véase https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_es

12. Véase, por ejemplo, www.banco.es

13. El protocolo de la capa de puertos seguros (SSL, secure socket layer) ha sido sustituido por las sucesivas versiones del protocolo de seguridad de la capa de transporte (TLS, transport layer security). Todos ellos son protocolos criptográficos que proporcionan privacidad e integridad en la comunicación entre dos puntos en una red de comunicación. De esta manera se garantiza que la información transmitida por dicha red no pueda ser interceptada ni modificada por quien no está autorizado para ello y solo los emisores y receptores legítimos tienen acceso a la comunicación de forma íntegra.

14. https://www.bbc.com/news/technology-30575104

15. Puede consultarse en https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional-2017

16. En https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme

17. En https://www.sogis.eu/

18. Para una información sobre la estrategia nacional de

ciberseguridad, DSN (2019).

19. Intentaremos a lo largo de este apartado mostrar los principales riesgos y amenazas que rodean a los usuarios de ordenadores personales. No obstante, dado que existen tantos aspectos a considerar y que no podemos abordarlos todos en este pequeño volumen, recomendamos al lector interesado que consulte bibliografía más extensa, como puede ser Vacca (2017b).

20. Para una visión global de la seguridad sobre los sistemas operativos Windows y Linux, respectivamente, véanse Scambray et al. (2008) y Herzog (2008).

21. Más información en https://gblogs.cisco.com/cansac/visual-networking-index-de-cisco-predice-el-triple-del-trafico-ip-para-2020/

22. Más información en https://www.311institute.com/hackers-are-using-your-photos-to-capture-your-fingerprints/ y https://www.elmundo.es/economia/2014/12/30/54a19eea268e3ec7718b4592.html

23. Más información en https://www.osi.es/es/actualidad/blog/2020/06/26/has-perdido-el-movil-cierra-sesion-en-tus-cuentas-por-prevencion

24. Véase https://opendatasecurity.io/what-does-metadata-disclose-in-photos/

25. Véanse CCN-CERT (2014); Vacca (2017b: parte IX, caps. 63-66; Vacca (2017a: sec. III, caps. 10-16), y NIST (2011a).

26. En https://aws.amazon.com/what-is-aws/

27. En https://elpais.com/tecnologia/2018/09/28/actualidad/1538153776_573 711.html y https://www.abc.es/tecnologia/redes/abci-facebook-y-cambridge-analytica-10-claves-para-entender-escandalo-robo-datos-201803 202237_noticia.html

28. Más información en https://www.ukessays.com/essays/information-technology/overview-of-the-equifax-data-breach.php

29. Un servidor DNS es un servicio que permite traducir una dirección web en la dirección IP (internet protocol) a través de la cual se localiza en Internet al servidor que contiene un cierto recurso. Dentro de una organización, es posible asignar nombres locales a las distintas máquinas de la red de la organización. El servidor DNS local permite asignar nombres de fácil lectura a las direcciones IP de las distintas máquinas.

30. La dirección MAC, también llamada dirección física, es un identificador de 48 bits formado por 6 bloques de dos caracteres hexadecimales, que corresponde de forma única a una tarjeta o dispositivo de red. Esta dirección es única para cada dispositivo y no depende del protocolo de conexión utilizado en la red.

31. En https://krebsonsecurity.com/tag/mirai-botnet/

32. En https://avancedigital.gob.es/es-es/Novedades/Documents/Plan_Nacio nal_Territorios_Inteligentes.pdf

33. Véase https://www.eldiario.es/hojaderouter/seguridad/contadores-inteligentes-seguridad-espana-hacking_1_4608231.html

34. Más información en http://www.startribune.com/pre-2013-medtronic-insulin-pumps-could-be-vulnerable-to-hacking/511906482/?refresh = true y https://www.medtronicdiabetes.com/customer-support/product-and-service-updates/notice11-letter

35. Véanse https://blackmarble.sh/zipato-smart-hub/ y https://labs.f-secure.com/blog/digital-lockpicking-stealing-keys-to-the-kingdom

36. Entendemos por nodo todo dispositivo incluido en una red de comunicación o de computación y que, por tanto, recibe y envía información de acuerdo con las características y objetivos de dicha red de comunicación o computación.

37. Véase https://www.lavanguardia.com/tecnologia/20180129/44364973910/strava-mapa-secretos.html

38. El firmware es un programa informático de más bajo nivel que

el propio software y que controla los circuitos electrónicos de cualquier tipo de dispositivo. De hecho, está muy integrado con la electrónica del dispositivo, siendo el software que tiene interacción directa con el hardware y, por tanto, el responsable de su control para que se ejecuten adecuadamente las instrucciones externas.

39. Véase https://www.semanticscholar.org/paper/Incorrect-HTTPS-Certi ficate-Validation-in-Samsung-Ghiglieri/77d9e9b73215f2246c2e435fde523bed542947b2

40. Shodan (https://shodan.io) es uno de los más conocidos motores de búsqueda que encuentra dispositivos IoT conectados directamente a Internet. Este buscador ofrece información sobre diferentes dispositivos.

41. Más información en http://www.cnpic.es/Preguntas_Frecuentes/Que_es_un_sector_estrategico_cuantos_existen/index.html

42. Para tener una visión cercana de lo que sucedió en España en 2018, véase el informe anual del CCN sobre amenazas y tendencias (CC-AyT, 2019) acerca de los diferentes tipos de atacantes, el tipo de acción llevada a cabo y sus víctimas; en la tabla 4 (CC-AyT, 2019) se incluyen los datos presentados en el citado informe.

43. La palabra vishing es un acrónimo de voice (voz) y phishing y es una estafa telefónica diseñada para que se proporcione información personal. El estafador, durante una llamada telefónica, hace uso de la ingeniería social para que el interlocutor comparta información personal, contraseñas y detalles financieros. De hecho, vishing es una forma de phishing si en la definición de este último incluimos el ataque mediante cualquier tipo de mensaje: correo electrónico, texto, llamada telefónica, chat, etc.

44. Más información en https://csirtsnetwork.eu/ y https://www.csirt.es/index.php/es/

45. Puede consultarse en https://www.abc.es/tecnologia/redes/abci-cambridge-analytica-facebook-cayo-careta-201903181122_noticia.html; https://elpais.com/internacional/2018/03/20/estados_unidos/1521574139

_109464.html y https://cnnespanol.cnn.com/tag/cambridge-analytica/

46. Algunas de las principales herramientas para la protección de la privacidad pueden verse con detalle en (ENISA, 2015, 2016) y serán tratadas con más detalle en el capítulo 4.

47. Véase https://www.privacytools.io/software/real-time-communication/

48. Véanse los principales protocolos de cifrado/descifrado en Hernández Encinas (2016).

49. En https://signal.org/docs/specifications/doubleratchet/

50. Véanse, por ejemplo, https://www.privacytools.io/providers/vpn/ y http://bestvpn.com

51. Véase https://netblocks.org/cost/

52. https://www.reuters.com/article/us-apple-china-malware/apples-ios-app-store-suffers-first-major-attack-idUSKCN0RK0ZB20150920

53. Véanse https://www.kaspersky.es/blog/35c3-spectre-meltdown-2019/17 620/ y https://www.xataka.com/seguridad/meltdown-y-spectre-asi-es-la-pesadilla-en-la-seguridad-de-las-cpus-de-intel-amd-y-arm

54. Consúltense https://cacheoutattack.com/ y https://lviattack.eu/

55. Más información disponible en https://www.incibe-cert.es/alerta-temprana/avisos-seguridad/vulnerabilidades-openpgp-y-smime-los-clientes-correo y https://www.xataka.com/seguridad/el-cifrado-pgp-en-peligro-esto -es-lo-que-deberias-hacer-para-estar-a-salvo-de-momento

56. En https://github.blog/2018-03-01-ddos-incident-report/

57. Habitualmente se denomina de esta forma a los piratas informáticos o hackers cuya actividad está dirigida a conseguir fines políticos haciendo uso de herramientas digitales ilegales o de

dudosa legalidad.

58. Véase https://www.academic-conferences.org/conferences/iccws/

59. Puede consultarse https://fas.org/irp/doddir/dod/jp3_13.pdf y https://www.act.nato.int/images/stories/events/2011/cde/rr_mnioe.pdf

60. En https://www.armyupress.army.mil/Portals/7/military-review/Archives/Spanish/MilitaryReview_20101031_art004SPA.pdf

61. SCADA (supervisory control and data acquisition) es un concepto que se emplea para desarrollar un software para ordenadores con el fin de supervisar, controlar y adquirir datos en procesos industriales a distancia.

62. Véase https://www.siliconrepublic.com/companies/softbank-arm-takeover-completed

63. Véase https://nvidianews.nvidia.com/news/nvidia-to-acquire-arm-for-40-billion-creating-worlds-premier-computing-company-for-the-age-of-ai

64. Más información en https://jorgegarciaherrero.com/guia-de-cookies-pestanee-eso-es-todo-gracias/

65. Véase https://nakedsecurity.sophos.com/2020/05/22/signal-secure-messaging-can-now-identify-you-without-a-phone-number/

66. Más información en https://receive-smss.com/ y https://sms24.me/

67. En https://www.privacytools.io/software/passwords/

68. En haveibeenpwned.com

69. Véase https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information

70. En https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know

71. El sitio https://downdetector.pe/ recoge los fallos de los principales servicios de Internet, siendo especialmente de interés comprobar los problemas que servicios como WhatsApp tuvieron durante la eclosión de la COVID-19, debido al uso masivo de esta aplicación para contactar con amigos y familiares en la fase de confinamiento.

72. En https://labs.bitdefender.com/2020/03/new-router-dns-hijacking-attacks-abuse-bitbucket-to-host-infostealer/

73. Véase https://threatpost.com/government-vpn-servers-zero-day-attack/ 154472/

74. Un trol es un agente humano que, de modo anónimo, interviene de modo provocativo en foros de discusión en redes sociales, blogs y otros contextos de intercambio de opinión en Internet. Los mensajes publicados por un trol están orientados a molestar y provocar una respuesta negativa por parte de los usuarios habituales de un cierto entorno de difusión de información en la red.

Índice de contenido

Ciberseguridad

Créditos

Introducción

Capítulo 1. Amenazas, vulnerabilidades y ataques

Malware

Suplantación de usuarios y robos de identidad

Denegación de servicio

Ingeniería social

Organizaciones de apoyo a la ciberseguridad

Capítulo 2. Dominios de la ciberseguridad

Ordenador personal

Dispositivos móviles

Computación en la nube

Internet de las cosas

Infraestructuras críticas

Capítulo 3. Ámbitos de uso

Gestión personal de la información

Gestión empresarial de los datos

Aspectos de la seguridad nacional

Capítulo 4. Soluciones y buenas prácticas de ciberseguridad

¿Software libre o software privativo?

Herramientas para proteger la privacidad

Protección de credenciales

Copias de seguridad

Uso de sistemas de detección de malware y actualización de software

Herramientas para la recolección de evidencias digitales y la auditoría de sistemas

Conclusiones. Principales desafíos de la ciberseguridad

Ciberriesgos y planes de continuidad en la era de la telesociedad

Confianza y fiabilidad tecnológica

Virus informacional: más allá de las fake news

Transición desde una inclusión pasiva en el ciberespacio hacia la constitución del cybernetes

Bibliografía

Notas